HACKER JOURNAL

Anno 2 - N. 31
31 Luglio - 28 Agosto 2003

**Boss:** theguilty@hackerjournal.it

**Editor:** grand@hackerjournal.it,

**Contributors:** Bismark.it, Piergiorgio Cardone, Nicola d'Agostino, Roberto "decOder" Enea, Lele, Norloz, Robin Hood, RoSwEIL,

**DTP:** Cesare Salgaro

**Graphic designer:** Dopla Graphic S.r.l.
info@dopla.com

**Copertina:** Zocdesign.com

**Publishing company**
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

**Printing**
Stige (Torino)

**Distributore**
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea



**HJ: INTASATE LE NOSTRE CASELLE**

**Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.**

**redazione@hackerjournal.it**

**hack·er (hãk'∂r)**

***"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."***

## PATENTE A PUNTI

Ogni tanto i miei neuroni fanno corto circuito, e i pensieri si mischiano. Stavo pensando alle nuove norme del Codice della Strada, quelle che hanno introdotto la "patente a punti", e mi è venuta in mente la patente europea del computer (European Computer Driving License, Ecdl). Per chi non lo sapesse, si tratta di un certificato che permette a chi lo consegue di dimostrare di avere confidenza con il computer, e saper svolgere i compiti principali: uso del sistema operativo (Windows) e dei programmi principali (Microsoft Office, Internet Explorer, Outlook...). Lasciamo per un momento da parte il fatto che per l'Ecdl esista un solo produttore di software, e non esistono sistemi operativi al di fuori di Windows (diamine, persino a Torino se uno prende la patente impara a guidare qualsiasi auto, e non solo una Fiat).

Stavo pensando a come sarebbe divertente se il meccanismo dei punti fosse applicato anche alla patente per i computer, e se – per esempio – a ogni violazione della netiquette corrispondesse una penalità...

Mandi a tutti i tuoi conoscenti ogni bufala che ti arriva per email? 3 punti (5 se lasci gli indirizzi in chiaro, nel campo cc:). Usi un client di posta che ti espone al rischio di inviare involontariamente dei virus? 5 punti. Sei un professionista del Web e realizzi siti che possono essere visti solo con un certo sistema operativo e un certo browser? Ti tolgo 7 punti. Sei uno spammer? Ritiro immediato.

Mi baloccavo un po' con questa idea, quando ho provato a pensare a cosa avrebbe significato nella pratica: un sistema di controllo e repressione attivo sul Web. E inoltre, c'è il rischio che anche per quanto riguarda la scelta dei "reati" e delle penalità, prevalgano gli stessi criteri di base su cui si fonda l'Ecdl: usi un sistema operativo "non omologato": ritiro della patente.

No, grazie: continuerò a sorbire vaccate inviate per email da qualche conoscente, a rinunciare a vedere alcuni siti perché il mio browser non visualizza comandi Html proprietari (azzi loro... perdono un visitatore), e purtroppo anche a subire la mia dose quotidiana di spam. E continuerò a spiegare più o meno gentilmente ai miei interlocutori come ci si comporta in Rete (molto spesso, i comportamenti scorretti sono solo frutto dell'ignoranza, nel senso letterale della parola). Vale la pena di sopportare qualche scocciatura in cambio di una Internet più libera.

***grand@hackerjournal.it***

FREE HACK NET

**ATTENZIONE!**
**Saremo di nuovo in edicola**
**Giovedì 28 agosto**
**BUONE VACANZE A TUTTI!**

# IL FREE-INTERNET DI HACKER JOURNAL




Vi abbiamo dato un sito ricco e con una comunità vivace, un canale Irc, poi un indirizzo email. Tutto ciò non vi basta? E allora registratevi subito per l'accesso a Internet targato Hacker Journal. In collaborazione con il provider Panservice siamo infatti lieti di offrirvi una connessione a Internet dalle caratteristiche uniche:

- **Connessione analogica e digitale ISDN, con possibilità di effettuare collegamenti multilink PPP fino a 128 Kbit/secondo.**
- **Possibilità di condividere la connessione con un router.**
- **Un indirizzo email del tipo: tuonome@hackerjournal.it con 5 Mb di spazio disponibile, e la possibilità di consultare la posta via Web o tramite il tuo programma di posta preferito.**
- **Utilizzo di filtri antispam sempre aggiornati, per una casella libera dalla spazzatura.**
- **Controllo antivirus sui messaggi email inviati e ricevuti.**
- **Server per newsgroup che permette di seguire i gruppi di discussione gerarchie it.*, italia.*, comp.*, europa.*, fido.ita.*, humanities.*, linux.*, macromedia.*, microsoft.*, misc.*, news.*, rec.*, sci.*, soc.*, talk.* e altri.**
- **Supporto agli utenti fornito attraverso una faq sempre aggiornata e un forum del nostro sito.**
- **Un nome che è una garanzia ;-)**

## COME COLLEGARSI

Per collegarsi, basta andare all'indirizzo

**www.hackerjournal.it/freehacknet**

e compilare il modulo di registrazione. Nelle pagine vengono indicati tutti i parametri necessari, che in ogni caso riportiamo qui:

| | |
|---|---|
| **Numero Telefonico** | **7020005073** |
| **Posta in arrivo (POP3/IMAP)** | **pop3.hackerjournal.it** |
| **Posta in uscita** | **smtp.hackerjournal.it** |
| **News server (NNTP)** | **news.hackerjournal.it** |

Chi ha già un indirizzo email@hackerjournal.it non ha bisogno di effettuare nuovamente la registrazione; basta che utilizzi il nome utente e la password della casella di posta. Il server smtp per la posta in uscita è valido solo se si effettua il collegamento attraverso il servizio di accesso di Hacker Journal. Chi utilizza altri servizi di accesso, dovrà continuare a usare il server Smtp del proprio provider.

## I COSTI DEL COLLEGAMENTO




Il collegamento ha il normale costo di una telefonata urbana. Come promemoria, ecco tutti i costi per ciascuna fascia oraria.

## Nuova password!

**Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.**

**user: ven3**
**pass: baril8**

HACKER JOURNAL



mailto:
redazione@hackerjournal.it



## SERVER-PALESTRA

L'altra sera stavo pensando a try2hack quando a un tratto... BUM!
Mi s'è accesa la lampadina: invece di trovare le password di try2hack perchè non organizzare un server linux (uno intero o una parte) come palestra?
Inizialmente ospiterà una home page che spiega le regole del gioco:
* Chiunque può introdursi nel server (se ne è capace) e impadronirsi del controllo di esso, migliorandone la sicurezza da lui violata.
* Finchè il server non verrà "rubato" da altri, l'hacker che ne detiene il controllo sarà padrone assoluto del server, con permessi illimitati.
* E' ammesso qualunque tipo di attacco al server al fine di prenderne il controllo.
* NON sono ammesse pornografia, pedopornografia e schifezze varie. Per i contenuti bisogna attenersi alle leggi in vigore, ma soprattutto al BUONSENSO!
E' possibile realizzare una cosa del genere?
Se il propietario del server NON sporge denuncia dopo ogni attacco, le forze dell'ordine interverranno comunque?
Ditemi cosa ne pensate!

**Freem**

***Abbiamo pensato a qualcosa del genere fin dai primi numeri, ma poi abbiamo scartato l'idea per vari motivi. Innanzi tutto, una volta preso il controllo del server, qualcuno potrebbe usarlo per fini illegali: potrebbe trasformarlo in "testa di ponte" per sferrare alri attacchi, per esempio. O usarlo per distribuire materiale illegale.***
***In secondo luogo, qualcuno potrebbe sferrare attacchi che non coinvolgono solo il server in questione, ma l'intera rete del provider che lo ospita (pensa a un attacco DoS). Visto che Linux è gratis, e che per un server senza grafica basta anche un PC molto vecchio, chi è seriamente interessato a studiare la sicurezza può organizzarsi un server-laboratorio in casa propria.***

## GUESTBOOK/1

appena preso il vostro giornale in edicola, per questione di abitudine ho subito letto il retro e sono rimasto perplesso... A parte il fatto che non credevo che il costo dei cd vergini fosse già aumentato, tanto che qualcuno li mandi a prendere addirittura all'estero per pagarli poco meno di 50 centesimi...
Mi rivolgo a chi ha proposto questa legge: non credete che aumentando il prezzo dei sudetti cd voi, in un certo senso, autorizziate le persone a violare i vostri diritti d'autore????
Non so se mi spigeo: è come se la legge dicesse ai ladri di banche: "ruba, ma mi raccomando versa il dovuto alla stato quando paghi le tasse.." bene, detto così, non sembra meno criminoso????!!!!!
Secondo me sì. Un'ultima cosa...: quando i lettori mp3 saranno totalmente diffusi tra la gente... cosa farete? aumenterete il prezzo dei cd fino a comparare la perdita di 20 cd audio???

**crash**

***In effetti, qualcuno sta avanzando parecchi dubbi sulla legittimità di questo provvedimento, e si stanno avanzando sospetti di incostituzionalità. Uno dei punti in discussione è proprio questo: il fatto di ottenere un compenso dalla vendita di ogni CD vergine a titolo di risarcimento per i danni causati dalla pirateria, non impedisce forse ai titolari del diritto d'autore danneggiati di esigere un ulteriore risarcimento quando i pirati vengono trovati davvero? Ai giuristi, l'ardua sentenza.***

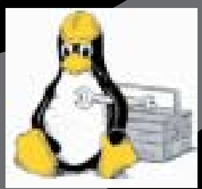
## GUESTBOOK/2

Nell'ultima pagina del n. 29 ho potuto leggere i commenti dei lettori al decreto legge che introduce la tassa sui CD-ROM vergini. Premesso che questo decreto non piace neanche a me, mi ha stupito vedere quei commenti su una rivista come la vostra, che pur criticando le leggi ha sempre cercato di far capire che queste vanno rispettate, e che cerca di promuovere un'idea etica dell'hacker. Come mai invece su questo punto avete pubblicato frasi così palesemente a favore della pirateria?

**Giacomo M.**

***Caro Giacomo, il guestbook è davvero quello che sembra: uno spazio libero e non censurato a disposizione dei lettori. Ci limitiamo a cancellare quelle risposte che violano in sé la legge (per esempio con contenuti diffamanti), ma per il resto pubblichiamo tutto. Anche quando, come in questo caso, non condividiamo la maggior parte dei messaggi.***

## FREE SOFTWARE, LA VERA RISPOSTA?



Premetto che non ho intenzione di giustificare il comportamento delle multinazionali. I prezzi sono troppo esorbitanti e dovrebbero condividere ciò che inventano, ma...c'è da trattare un argomento ben maggiore della conoscenza informatica. Caro lettore, secondo te, ad una povera vecchietta ignorante di computer con una misera pensione, fa-

# www.hackerjournal.it

## ☺ Tech Humor ☺

1 Comando o nome di file errato! Vai in castigo nell'angolo.

2 Messaggio di Windows: "Errore di salvataggio del file!Formattare il disco fisso adesso?"

3 File non trovato. Me lo invento? (S/N)

4 Runtime error 6D at 417A: 32CF: user incompetente.

5 Windows VirusScan 1.0- "Trovato Windows: Rimuoverlo? (S/N)

6 La cartella specificata non esiste. Contattare Invicta? (S/N)

7 Il programma "Netscape Communicator" ha provocato il sistema operativo. Reagire? (S/N)

8 Premere Invio per terminare il processo, $ per corrompere i giurati.

9 Memoria insufficiente ad eseguire... che stavo scrivendo?

10 Operazione riuscita. Se la situazione persiste, contattare il fornitore del sistema operativo.

11 I disco nell'unità CD-ROM non mi piace. Non hai nulla di meglio?

12 Tastiera non collegata. Premere F1 per continuare.

**(segnalato da Tommy V.)**

rebbe più comodo avanzare le proprie conoscenze su nuovi algoritmi di calcolo o pagare meno tasse? Cosa centra, mi chiederai, giusto? Calcola che le multinazionali sono delle aziende e come tali cedono una parte dei loro profitti allo stato, oltre che a fornire nuovi posti di lavoro. Questo significa far muovere l'economia, aiutare quella povera vecchietta a pagare meno tasse, trovare un lavoro ad un programmatore senza speranza. Quello che andrebbe sensibilizzato non è tanto l' incetivo al free software; il fenomeno ci sarebbe comunque, stesso da parte di programmatori che lavorano per le multinazionali, perchè free software è un sentimento che si sente dal profondo del cuore...condividere ciò che si scopre. Ciò che andrebbe realmente valorizzato è il mettere in pratica quello che ti ho appena descritto qui! Rendere più accessibili i prezzi! Ecco come si combatte la pirateria! Altro che alzare il prezzo dei cd vergini!!!
In conclusione... non sminuiamo le multinazionali pensando a come le possiamo distruggere utilizzando semplicemente codice free, ma come potrebbero essere utili alla società! Ricordate che i problemi economici sono ben maggiori della conoscenza fine a se stessa sopratutto per le persone che della conoscenza non gliene fotte un bel niente. Lo scopo è di equilibrare questi due grandi fabbisogni, senza sminuirne l'uno o l'altro.

**Aurelio e Danilo**

***Una cosa di cui non tieni conto è che la maggior parte dei soldi pagati a una multinazionale del software finisce all'estero; tante piccole aziende che invece si occupano di installare, sviluppare e fare assistenza per il software libero, porterebbero ben più vantaggi all'economia italiana, sia in termini di posti di lavoro, che di tasse versate.***

### POSTA IN VACANZA

Salve!Per un po di tempo non avrò a disposizone il mio PC,quindi per controllare le e-mail mi devo recare ad un Internet Point,collegarmi al sito del mio provider e leggere la posta via Web.Tutto questo è sicuro?Voglio dire,non è che un soggetto può recuperare la password(che ho digitato sul sito del mio provider) che si è andata a registrare in qualche meandro di Windows?Quali accortezze mi consilgiate?

**Matteo D.**




***Come prima cosa, se il servizio Webmail che utilizzi permette l'uso di connessioni sicure (https), sfrutta questa possibilità. Yahoo per esempio lo consente, anche se limitatamente allo scambio delle password (qualcuno potrebbe comunque intercettare le pagine con i messaggi).***
***In alternativa, puoi crearti un'email sul servizio HushMail (www.hushmail.com), che offre appunto la possibilità di consultare una casella di posta in modo assolutamente sicuro. Hushmail funziona grazie a una piccola applicazione in Java che viene scaricata ed eseguita dal browser; quest'applicazione si occupa di cifrare tutte le comunicazioni da e verso il server, garantendo la massima riservatezza. Per scrupolo, alla fine elimina i file temporanei di Internet (cioè pulisci la cache del browser), e cancella la Cronologia.***

### ABBIAMO TOPPATO...

Nell'articolo "Il bug della format string" pubblicato sul n. 30 abbiamo scritto che lo stack parte da 0xbffff000, ma in realtà inizia da 0xbfffffff. C'è poi un errore nella firma dell'articolo, l'indirizzo dell'autore è: bugsman@libero.it.

Dobbiamo poi precisare un'altra cosa: l'articolo "L'arte dell'inganno" pubblicato sul n. 29 è in gran parte ispirato da un white paper dal titolo "Social Engineering: una guida introduttiva", scritto da Andrea "Pila" Ghilardini e pubblicato sul sito dell'associazione Italian Black Hats (http://www.blackhats.it/it/papers/social_engineering.pdf).
Vi invitiamo a leggere anche il testo originale, molto più completo e dettagliato.

# NEWS



## NUMERI

### I NUMERI DELLA PIRATERIA

La Gaurdia di Finanza e la Business Software Alliance (BSA) hanno portato a termine l'operazione Corsaro, effettuata su 400 soggetti economici controllati su tutto il territorio nazionale, che ha dato questi risultati:

**240:**
Soggetti economici risultati irregolari

**3.000:**
Programmi software installati senza licenza

**4.700:**
CD masterizzati

**424:**
Pacchetti software contraffatti

**1.034:**
PC sequestrati

### PER QUEL CHE RIGUARDA LE ATTIVITÀ DI CONTROLLO CONDOTTE DALL'INIZIO DELL'ANNO:

**3.016:**
Interventi effettuati

**2.300:**
Persone denunciate (di cui 81 in stato di arresto)

**1 MILIONE E 500.000:**
Supporti audiovisivi sequestrati

## BUFALE TRUFFALDINE



Che tra i prati della Rete e della posta elettronica pascolino indisturbate bufale di tutte le specie e va beh, ci siamo abituati. Poco male. Al massimo piangiamo come vitelli per le improbabili storie strappalacrime che raccontano, o facciamo la figura dei boccaloni, rigirandole a chi più sgamato di noi ha già capito tutto. Ma che le succitate bestie pallifere si mettano anche a battere cassa è una vera seccatura. L'ultima tra le bufale, che oltre a farci fessi pretende dei soldi, riguarda ICQ. La truffa si presenta sotto forma di un messaggio proveniente da Icq stesso che ci ricorda che dopo tanti anni di servizio gratuito, questo programmino di chat diventa a pagamento. Oltre ad invitarci a versare un contributo, ci viene chiesto di compilare un modulo con nostri dati personali carta di credito compresa. Chi non paga, intima il messaggio minaccioso, vedrà il proprio account cancellato da ICQ. Nel caso ci fosse bisogno di dirlo, non molliamo niente: è una truffa.

## CELLULARE O INCUBO?



Il cellulare sta diventando veramente qualcosa di impossibile. Non solo se lo tieni acceso ti condanni a essere rintracciabile sempre e ovunque e a inviare informazioni sui tuoi spostamenti ai ripetitori vari. Adesso anche se giace spento e silente nel più remoto angolo della tua borsa è in grado di trasmettere segnali che, decodificati, stabiliscono la tua posizione con un minimo margine di errore. Quantomeno se vivi in Gran Bretagna. Questo tipo di informazioni fino ad ora accessibili solo dalla polizia, potrebbero essere presto alla portata anche di datori di lavoro e operatori commerciali. Così per esempio una società di commercio potrà controllare dove si trovano i suoi rappresentanti, oppure ristoranti o locali saranno in grado di inviare messaggi promozionali a potenziali clienti nei paraggi. Speriamo che una simile diavoleria non attraversi mai la Manica. Dire che è inquietante è dire poco.

## A VOLTE RITORNANO

Gli hacker over "anta", quelli della prima generazione, tornano all'attacco. I loro metodi non sono certo aggiornatissimi, ma i danni li fanno lo stesso. Da un recente rapporto dell'US Department for Homeland Security pare che stiano aumentando gli atti di phreaking, cioè gli attacchi pirati sferrati attraverso le reti telefoniche. Una simile strategia non è certo motivata da strani rimpianti per i vecchi metodi. Il fatto è che la politica di protezione delle aziende concentra i suoi sforzi sulla rete informatica, lasciando quasi praticamente sguarnita quella telefonica. E si sa: ogni breccia per un hacker è un invito a entrare. Aziende correte ai ripari.



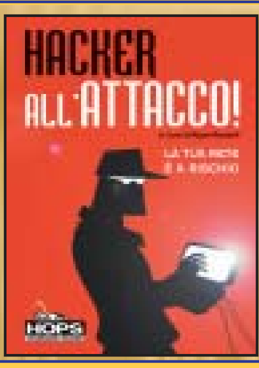
## ARROTONDARE LO STIPENDIO

Chi lavora in Microsoft guadagna bene, si sa. Soprattutto se decide di arrotondare lo stipendio con una buona dose di iniziativa e spirito imprenditoriale, come ha fatto un tale Richard Gregg. Questo dipendente, sfruttando la sua posizione nell'azienda, acquistava grossi quantitativi di software a prezzi vantaggiosi che poi rivendeva all'esterno. Il business gli è fruttato nell'ordine: 17 milioni di dollari, il licenziamento in tronco e un procedimento legale. Complimenti Richard!




## IL LIBRO DELL'ESTATE

"Hacker all'attacco! La tua rete è a rischio", un nome un programma per un libro che quest'estate non può mancare sotto l'ombrellone o sul comodino di tutti gli hacker. Si tratta di una raccolta di racconti scritti da hacker doc, dove tra gli intrecci e personaggi di fantasia si svelano tecniche e tecnologie assolutamente reali. Metodi di attacco, contrattacco,




rotte del pensiero degli hacker. Ma non vorremmo toglervi la suspence raccontandovi troppo. Il volume sarà in libreria dal 25 luglio e ordinabile dal sito di Hops Libri (www.hopslibri.it) già dal 15 luglio. I lettori di Hacker Journal che accedono al sito di Hops Libri attraverso il link pubblicato sul nostro sito, risparmieranno un bel 15% sul prezzo di copertina

## STRIP TEASE ALL'AEROPORTO



Va bene che rischiare di volare chiappa a chiappa con un possibile dirottatore non è affatto bello, ma anche sfilare più o meno come mamma ci ha fatti sotto gli occhi della polizia, non deve essere il massimo della vita. Di cosa stiamo parlando? Di un nuovo dispositivo di sicurezza prossimamente in dotazione alla polizia degli aeroporti americani che controlla se abbiamo addosso qualche arma o ordigno sospetti. Il problema di questo super scanner a raggi X è che restituisce a monitor un'immagine della persona scansionata, completamente nuda. Ora, se un re del passato disse che "Parigi val bene una messa", certamente la sicurezza varrà bene uno spogliarello, però... che vergogna. Per ovviare ai problemi di privacy pare che siano al vaglio possibili soluzioni che prevedono il posizionamento di una... foglia di fico elettronica là dove non batte il sole. L'aggeggio si chiama backscatter, costerà circa centomila dollari e potrebbe essere impiegato in tutti gli aeroporti a stelle e strisce già dal prossimo anno.

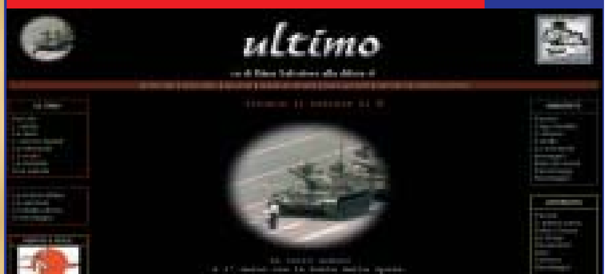
# HOT!

## IL PINGUINO E IL MAXI SCHERMO



Linux ormai la fa da padrone un po' ovunque. La sua ultima conquista è il mondo del cinema. La DreamWorks ha infatti annunciato che il nuovo film di animazione "Sinbad: the Legend of the Seven Seas" è stato interamente realizzato su piattaforma Linux. La casa di produzione americana assicura che intende bissare realizzando con la stessa piattaforma il suo prossimo film di animazione Shrek 2. Per Linux comunque non è la prima volta nel mondo del cinema: è stato infatti utilizzato anche per altri film, tra cui Harry Potter e Scooby-Doo.

## CAPITANO ULTIMO




Vogliamo segnalare un sito alternativo che deve il suo nome a una persona che ha dedicato al vita alla lotta contro la mafia, Il Capitano Ultimo. Oltre alla sezione antimafia, ce ne sono di altre davvero interessanti: una dedicata all'ambiente, una alla poesia, una agli artisti di strada, una ai writers metropolitani, un'altra ancora agli Apaches. Tantissime sono le notizie e i materiali a nostra disposizione. Da non perdere le pagine dedicate agli Hacker, con segnalazione di film, libri, articoli. Insomma una voce un po' fuori dal coro che merita una visita e anche più d'una.

# NEWS

## SITI WEB

### GNOCCHE E ARMI CHIMICHE

www.google.it




Simpatico scherzetto su uno dei motori di ricerca più diffusi. Si tratta di Google e per scoprire l'arcano è sufficiente digitare la scritta "Weapons of mass destruction" nello spazio per la ricerca e cliccare sul pulsante "Mi sento fortunato". Poi provate anche con "trombare la gnocca".

### MATRIX PING PONG

www.ntv.co.jp/channel/kasoh



Un sito giapponese con una serie di divertentissimi filmati come, per esempio, il gioco del ping pong stile matrix...con tutti i retroscena dei trucchi utilizzati.

### L'ORIGINALE PUBBLICITÀ DELLA HONDA

http://users.pandora.be/soulwaxke/honda-ad.html



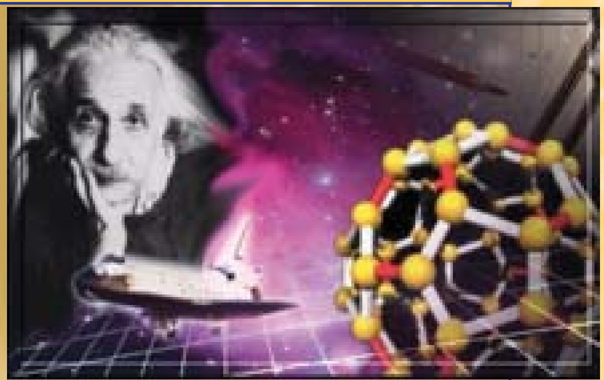
Un percorso a ostacoli per la nuova pubblicità della Honda, da seguire dall'inizio alla fine tutto d'un fiato.

## IL PAPÀ DI NAPSTER SI CONVERTE




Shawn Fanning, il ventiudenne creatore di Napster, a quattro anni dall'invenzione del servizio di file-sharing più famoso del mondo, ha deciso di immolarsi al dio denaro e costringere chi scambia su Internet brani protetti da copyright a pagare i diritti d'autore. Per fare questo, vorrebbe sviluppare una tecnologia in grado di analizzare la traccia audio di ogni brano scambiato online e di confrontarla con un database di tutte le canzoni protette da copyright. In caso di corrispondenza positiva, il sistema chiederà all'utente di pagare e si incaricherà di girare l'importo a chi detiene il diritto d'autore. Il sistema funzionerà solo se sarà appoggiato dalle case discografiche e dai servizi di file-sharing più utilizzati.

## PLANETLAB, UN NETWORK PER LA RICERCA



Gli scienziati di quattro continenti saranno collegati grazie a PlanetLab (www.planet-lab.org), un network ideato per testare e verificare nuovi servizi via Internet. Sponsor dell'iniziativa: Intel e Hewlett-Packard. Europa, Stati Uniti, Asia e Australia sono i quattro Paesi coinvolti nel progetto, che ha lo scopo di testare e verificare il funzionamento di nuovi servizi Internet senza gravare sulla Rete attuale, ma sfruttandola comunque per i collegamenti fra istituzioni scientifiche. Si tratta di una rete formata per il momento da 160 PC gestiti in 16 diversi paesi da 65 nodi operativi, in grado di inviare e trasmettere dati in simultanea tra molteplici utenti. Il tutto basato sul sistema operativo Linux. I progetti che per ora si sono avvalsi della rete riguardano il peer-to-peer, la mappatura di rete e soprattutto la sicurezza: attraverso PlanetLab si conta infatti di individuare molto più velocemente di quanto fatto fino ad ora la diffusione di virus informatici o l'avvio di un attacco DDoS (distibuted denial-of-service), volto a disabilitare uno o più sistemi operativi online.

## IN ARRIVO IL KERNEL 2.6 DI LINUX



E' stata portata a termine da Linus Torvalds la versione 2.5.75 del kernel di Linux. A detta di Torvalds, questa dovrebbe essere l'ultima della serie. Il kernel 2.5, un progetto di sviluppo finalizzato a sperimentare le nuove tecnologie, verrà integrato nel kernel 2.6 per essere utilizzato nei prodotti finiti.Lo sviluppatore ha dichiarato che il lavoro su una versione test del kernel 2.6 sta per iniziare. "Vi conviene segnarvi questa versione, perchè probabilmente sarà l'ultima appartenente alla serie 2.5" ha scritto lo sviluppatore in una mailing list formata da sviluppatori di kernel. Torvalds ha aggiunto che lui e lo sviluppatore Andrew Morton hanno intenzione di cominciare una serie pre-2.6 in cui sarà piuttosto complicato inserire delle patch.

## UN VIRUS TRASFORMA I PC IN SERVER PORNOSPAM



Forse è un russo l'autore di un trojan horse che ha infettato i computer di circa duemila utenti Internet connessi a banda larga. Pare che il virus, battezzato Migmaf, entri in alcuni sistemi Windows e piazzi quello che sembra essere un proxy server invertito. L'autore utilizza i server degli utenti venutisi così a creare per inviare tonnellate di spam pornografico con cui pubblicizza siti russi che offrono pornografia a pagamento. La possibilità di nascondersi dietro ai computer degli utenti infetti ha finora consentito all'autore non solo di non farsi individuare, ma anche di impedire ai provider e ai servizi antispam di bloccare con efficacia lo spam, che appare spedito da IP che appartengono a semplici utenti e che cambiano di continuo. L'IP del server master da cui parte la pagina spedita al computer infetto viene inoltre cifrato con un algoritmo che ne rende estremamente complessa l'individuazione.
Ed è probabile che il server cambi IP con una certa frequenza, proprio per evitare intercettazioni. L'analisi del fenomeno, effettuata da LURHQ, è disponibile all'indirizzo:

www.lurhq.com/migmaf.html

## IL WI-FI A SOSTEGNO DELLE NAZIONI POVERE



Il Wi-Fi può avere grande impatto economico soprattutto nelle nazioni in via di sviluppo. E' quanto ha dichiarato il segretario generale delle Nazioni Unite Kofi Annan durante una conferenza dedicata al digital divide. Secondo Annan, il Wi-Fi consente di sviluppare una rete wirelelss con costi di installazione e gestione molto inferiori a quelli di tutte le altre tecnologie senza fili. E questo soprattutto nei paesi in cui non esistono valide infrastrutture di comunicazione. Unico ostacolo: la resistenza di molti governi locali, che sono spesso contrari all'utilizzo di tecnologie che usano parti libere e non regolate dello spettro radio.

## TAGLI ALLE TARIFFE 709

0,06 euro. Questo il prezzo massimo al minuto che un servizio fornito attraverso numerazione 709 può imporre all'abbonato secondo il Piano di Numerazione Nazionale approvato dall'Autorità TLC. Penalizzati quindi i fornitori di dialer, che fino a questo momento facevano pagare fino a 3 o più euro al minuto per l'offerta di loghi, suonerie e quant'altro. Inoltre, l'Autorità ha stabilito anche che lo scatto alla risposta non potrà superare gli 0,10 euro. I servizi che caricano una tariffa per la fornitura di servizi di informazione o di intrattenimento, verranno forniti attraverso la numerazione 892 quando la loro natura sarà di tipo sociale-informativo. In questo caso lo scatto alla risposta non potrà essere superiore agli 0,3 euro e ogni minuto di servizio non potrà superare gli 1,5 euro.

## HOT!

## CRIMINI INFORMATICI



Secondo i dati raccolti da alcuni esperti di sicurezza, gli attacchi criminali alle reti di computer tendono a raddoppiare ogni anno e mezzo in quanto a diffusione e pericolosità. In particolare, la National High-Tech Crime Unit, un centro di ricerca inglese specializzato in sicurezza, dopo un'indagine durata tre anni che ha esaminato un campione di 370 imprese attive in Gran Bretagna, è giunta alla conclusione che la quantità di attacchi criminali è sistematicamente aumentata, nel Regno Unito, di oltre il 100% ogni anno a partire dal 1999. Pare che lo scorso anno solo il 3% delle imprese britanniche sia rimasto immune da attacchi esterni e un terzo delle aziende non prevede alcun piano per contrastare seriamente un attacco informatico. In ordine di importanza, per grado di pericolosità, vi sono le frodi finanziarie, le infezioni dei virus e gli attacchi denial of service. Inoltre, la ricerca ha rivelato come, negli ultimi dodici mesi, il furto di computer portatili aziendali sia uno dei crimini informatici più diffusi, che sfiora addirittura il 77%.

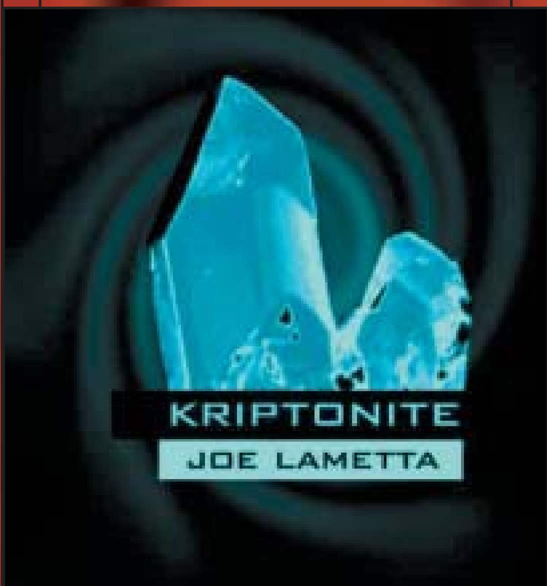
## I PC DI SUSE LINUX

Microtel, produttore specializzato in PC a basso costo, ha lanciato una nuova linea di PC economici dove si trovano preinstallate la distribuzione Linux di SuSE e sulla suite per l'ufficio OpenOffice. I nuovi PC vanno ad affiancarsi a quelli basati su LindowsOS. Per 298 dollari è possibile portarsi a casa un computer dotato di processore Duron 1,2 GHz, 128 MB di RAM, 20 GB di hard disk, drive CD-ROM, scheda di rete Ethernet, modem 56K, tastiera, mouse e casse audio. La gamma di computer basati su SuSE Linux comprende anche modelli basati su Athlon XP, Celeron o Pentium 4 ed equipaggiati con masterizzatore e/o maggiori quantità di memoria o spazio disco. Per il momento questi PC possono essere acquistati solo in USA. SuSE si è tuttavia detta fiduciosa di poter raggiungere, in futuro, una partnership con Wal-Mart per la distribuzione di PC Linux anche sul mercato europeo.

# Spedire email anonime

**L'unico vero modo per spedire email in modo che non sia possibile risalire al mittente, è quello di usare dei remailer anonimi. Ma può essere meno facile di quel che sembra.**

Quando ci chiediamo se esiste davvero un posto in cui si possa esprimere liberamente il proprio pensiero, sicuramente la risposta è una sola: Internet.
Nonostante la sua "infanzia militare", infatti, la Rete ha alcune caratteristiche per rappresentare quel modello di **libertà d'espressione che tanta gente per secoli ha sognato**. Ma se guardiamo il fenomeno con un occhio un po' più attento ci rendiamo conto che la realtà dei fatti non è davvero così rosea come sembra. Anche in Rete, purtroppo, sopravvivono ancora dei concetti di gerarchia e controllo che si possono tradurre in rappresaglie più o meno forti nei confronti dell'autore di alcuni pensieri e informazioni. Immaginate un dipendente che rende pubblica su Internet la notizia che l'azienda per cui lavora non segue le procedure di sicurezza per lo scarico di rifiuti tossici: **nel giro di poco il Grande Fratello informatico individuerebbe l'impiegato che subirebbe ritorsioni da parte della dirigenza**. Quest'esempio ci fa capire che per avere una vera libertà di pensiero in rete, dobbiamo comunque trovare un modo per restare anonimi. Per quanto riguarda le comunicazioni via e-mail, nacque il concetto di **remailer anonimo**, ossia un servizio che permetteva di mandare mail di cui non fosse individuabile il mittente.




Kriptonite è un libro molto interessante che spiega i principi base della crittografia e dell'anonimato in Rete. È un po' vecchiotto, e molti dettagli non sono più validi, ma per una infarinatura è ottimo. Lo potete leggere online o scaricare da www.ecn.org/kriptonite/

## >> Non vedo, non sento, ma parlo

In principio fu anon.penet.fi, forse il più famoso tra i primi remailer anonimi. Purtroppo questo remailer chiuse i battenti quando **le autorità finlandesi costrinsero il suo amministratore a rivelare la vera identità di uno degli utenti del servizio**. Questo avvenne perché anon.penet.fi era uno di quelli che vengono definiti **pseudo-anonymous remailer**. Questo significa che il servizio permetteva di creare un account con uno pseudonimo e usarlo per inviare e ricevere mail, quasi come succede ora con servizi come yahoo e hotmail. In questi casi l'amministratore del servizio conosceva comunque i dati di ogni utente iscritto. I difensori dell'anonimato avevano imparato una nuova lezione: **non bisogna confidare sull'occultamento dei dati da parte di un admin**. Sorsero così i primi veri remailer anonimi. Il concetto alla base di questi remailer è quello di non loggare le operazioni e di sostituire l'header della mail (che contiene infor-

# LE CATENE DI REMAILER




La massima sicurezza viene garantita solo dall'uso di più remailer in catena (di solito tre). In una catena di remailer, il messaggio originale viene cifrato più volte con le chiavi dei vari remailer, aggiungendo le istruzioni per l'invio al destinatario successivo (altro remailer o destinatario finale). In questo modo, anche se la sicurezza di uno o due dei remailer fosse compromessa, non sarebbe comunque possibile ricostruire il passaggio del messaggio dal mittente al destinatario.
In pratica, funziona così:

**1** Il primo remailer riceve un messaggio, cifrato con la sua chiave, che contiene le istruzioni per inviare anonimamente il messaggio al secondo remailer; il resto del messaggio è cifrato con la chiave del secondo remailer. Il primo remailer conosce solo il mittente e l'indirizzo del secondo remailer. Il corpo del messaggio da inoltrare è comunque cifrato, con la chiave del secondo remailer.

**2** Il secondo remailer riceve la mail dal primo, la decifra e al suo interno trova in chiaro le istruzioni per inviare il messaggio al terzo remailer, più il corpo del messaggio, cifrato con la chiave del terzo remailer (che lui non può aprire). Il secondo remailer non sa da chi arriva la mail (l'ha ricevuta dal primo remailer), né sa a chi è destinata (la spedisce al terzo remailer).

**3** Il terzo remailer riceve un messaggio dal secondo remailer; lo decifra, e trova le istruzioni per inviarlo in modo anonimo al destinatario finale. Se anche il messaggio finale è cifrato (cosa buona e giusta), il terzo remailer non avrà alcuna possibilità di stabilirne il contenuto, né tanto meno di risalire al mittente.

mazioni sul mittente) con un altro header "fasullo" e inviare al destinatario la mail così modificata.

## >> Remailer Cypherpunk

La prima generazione di remailer anonimi viene definita **Type I**, in gergo **Cypherpunk remailers**.
Supponiamo di voler inviare una mail anonima a pippo@pluto.it usando un remailer Cypherpunk: scriviamo una mail contenente questo testo:

```
::
Anon to: pippo@pluto.it
Latent-Time: +0.00

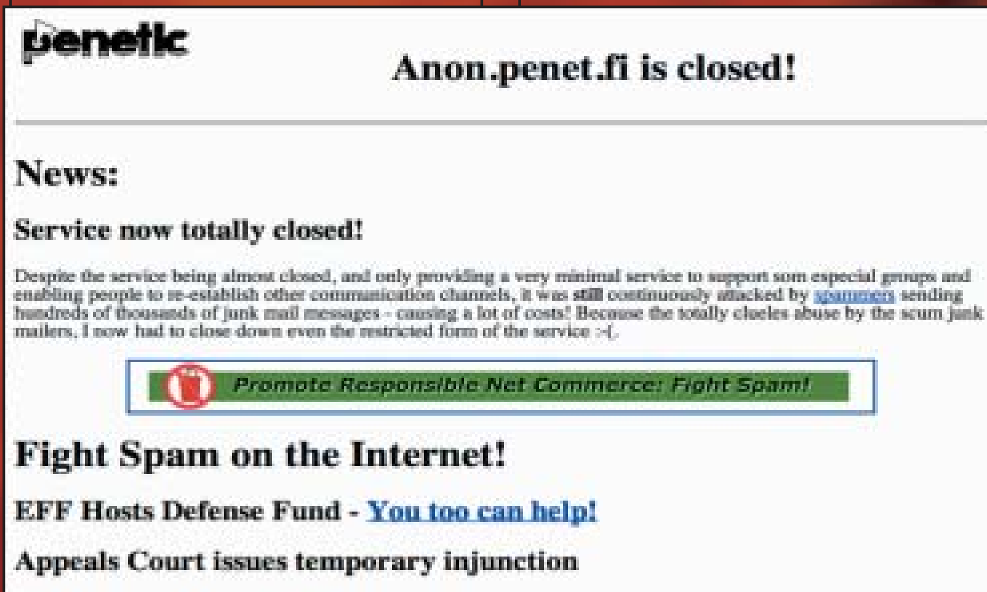
##
Subject: oggetto della mail

Testo della mail
```

Dobbiamo poi inviare questa mail non a pippo@pluto.it ma all'indirizzo del remailer, poi sarà lui a provvedere al corretto invio della posta. Il ricevente vedrà una mail che arriva da un indirizzo riconducibile al remailer ma non al vero mittente.
Molti remailer Cypherpunk accettano ormai **solo mail codificate con PGP**: in questo caso dobbiamo ottenere la chiave pubblica PGP del remailer mandandogli una mail vuota con oggetto "remailer-key" e otterremo una risposta con la chiave che ci serve. Codifichiamo il messaggio precedente con la chiave PGP ottenuta e, prima di inviare il testo cifrato al remailer, aggiungiamo in testa queste due righe:

```
::
Encrypted: PGP
```

Giocando un po' con i blocchi Anon to



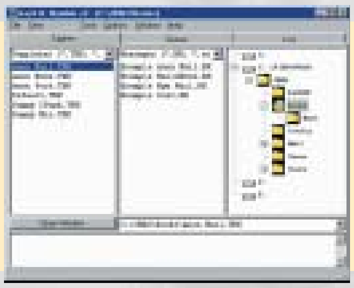

Anon.penet.fi è stato uno dei primi remailer, e sicuramente il più famoso. Ha ridotto drasticamente le attività dopo che è stato costretto a rivelare il mittente di un messaggio sulla chiesa di Scientology, inviato in un newsgroup. Dopo che è stato pesantemente preso di mira da spammer di tutto il mondo, ha chiuso definitivamente bottega.

# SPEDIRE MAIL ANONIME CON JACK B. NIMBLE

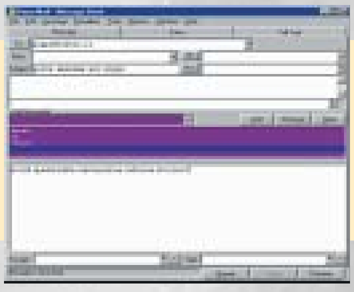
Come avrete notato, scrivere dei messaggi in un formato accettabile da un remailer non sempre è facile, e nel caso del Mixmaster è quasi impossibile, quindi sono stati realizzati molti client che automatizzano la procedura. Utilizzando questi programmi scrivere una mail anonima diventa invece semplice come scrivere una normalissima mail. Prendiamo come esempio uno dei migliori client per Windows, chiamato Jack B. Nimble (JBNv2). Questo programma in realtà non è altro che un front-end per PGP e per il protocollo mixmaster, ed è necessario installarli. Abbiamo bisogno di PGP con supporto RSA (vedi box link). Scarichiamo l'eseguibile, installiamo, creiamo le nostre chiavi, dopodiché apriamo PGPKeys, facciamo un Ctrl-T e abbiamo davanti il menu delle preferenze. Assicuriamoci che l'opzione Always Encrypt to default keys NON sia selezionata, ed usciamo. Ora abbiamo bisogno di mixmaster: scaricate lo zip dall'indirizzo che trovate nel box ed estraetelo nella cartella c:\mix .
A questo punto non ci resta che scaricare il nostro JBN (solito box dei link) e.. via col setup! Quando l'installazione sarà terminata, dovremo configurarlo: connettiamoci alla rete e lanciamo JBN. Ci verrà subito chiesto quale versione di PGP usiamo, e noi dobbiamo cliccare il bottone "PGP 5.5.3x/6.x". Poi dobbiamo indicare in che cartella abbiamo installato mixmaster (nel nostro caso c:\mix) e alla successiva richiesta cliccare yes solo se abbiamo una connessione dialup. Ora JBN si metterà al lavoro per scaricare liste di remailer e relative chiavi. Qui cliccate Ok o Yes ad ogni richiesta (sono solo segnalazioni di remailer o chiavi non trovate) e attendete che si apra una finestra MS-DOS che serve a configurare mixmaster. Qui l'unica cosa che dobbiamo fare è inserire per due volte una sequenza casuale di 128 tasti.



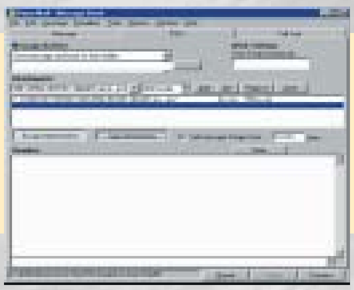
Infine in JBN andate nel menu Window e cliccate Send Profiles. Ora nella schermata che compare dobbiamo abilitare la casella Enabled, inserire un nome a piacere in Profile Nickname, il nome del nostro server di posta in uscita in SMTP Server e il nostro indirizzo reale di posta in From header, e premere OK. Abbiamo passato un po' di tempo a installare e configurare il tutto, ma ne è valsa la pena perché siamo finalmente pronti ad inviare mail anonime. Basta fare doppio clic sul template chiamato Anon mail.TBK nella finestra principale di JBN.



Così facendo apriremo una finestra molto simile alla finestra Nuovo messaggio di Outlook. Riempiamo i campi To, CC e BCC con i destinatari e il campo Subject con l'oggetto della mail. Lasciamo vuoto il campo Nym e cancelliamo dallo spazio sottostante gli header che non ci servono (in genere From e References) altrimenti la nostra mail non sarà elaborata correttamente. Notiamo ora una casella verde con tre scritte AUTO. Selezioniamole ad una ad una e cambiamole usando la ListBox appena sopra: questi sono i remailer da mettere in catena. Se lo sfondo è verde stiamo usando remailer Cypherpunk, mentre per passare ai Mixmaster aprite il menu Remailers e cliccate su Mixmaster e la casella remailer diverrà magenta. Effettuate la stessa operazione se volete tornare ai Cypherpunk.



Scegliete almeno due o tre remailer per avere più sicurezza. Ora basta scrivere il testo della mail nella casella grande e premere il bottone Queue per mettere la mail nella coda di invio. Possiamo anche firmare o criptare la mail con PGP usando le ListBox Encrypt e Sign e scegliendo la chiave che vogliamo usare. Per inviare le mail in coda, dalla finestra principale di JBN cliccate sulla "paletta" Queue e poi premete il bottone Send. Non vi spaventate se vedete più mail di quante ne avete scritte, a volte le mail troppo lunghe vengono spezzettate in vari frammenti.



Possiamo anche allegare file: per farlo, nella finestra di creazione messaggio cliccate sulla "paletta" Extra. Qui cliccate sul bottone con l'asterisco vicino alla casella attachments e scegliete i file da inviare. Poi scegliete la codifica (in genere Mime auto oppure UUEncode) e cliccate Add. Possiamo anche criptare e firmare gli allegati premendo i tasti Encrypt Attachments e Sign Attachments.

e la codifica PGP possiamo anche forzare la mail a **passare attraverso una catena di remailer**, ottenendo quindi una maggiore sicurezza (vedere il box a riguardo).



Ok, sembra che abbiamo raggiunto il nostro scopo e cioè rimanere anonimi. In realtà ci sono molti attacchi effettuabili su un remailer Type I, soprattutto se possiamo analizzare il traffico in ingresso ed in uscita, perché le mail vengono inviate nello stesso ordine in cui arrivano e potremmo fare un'analisi delle dimensioni dei pacchetti. In pratica, chi potesse osservare il traffico in potrebbe notare che una mail di 150 Kbyte viene inviata da noi al remailer, e a un certo intervallo di tempo una mail di 150 Kbyte viene inviata dal remailer al vero destinatario, e **facendo due più due individuare mittente e destinatario del messaggio**.

## >> Remailer Mixmaster

Tutte queste considerazioni hanno portato allo sviluppo dei remailer Type II chiamati anche **Mixmaster remailer**. I remailer Mixmasters non usano la codifica PGP ma una codifica propria, basata su una chiave chiamata Mix-key e ottenibile nello stesso modo di una chiave PGP Cypherpunk. Il messaggio ricevuto viene codificato più volte con gli algoritmi RSA e Triple-DES e passato attraverso una catena di Mixmaster. Ogni remailer rimuove uno "strato" di codifica, fino all'ultimo che decifra completamente il messaggio e lo invia al destinatario. Per evitare gli inconvenienti del Cypherpunk, i Mixmaster **mescolano l'ordine di uscita delle mail e le suddividono in tanti pacchetti della stessa dimensione**. Inoltre ogni remailer della catena (a parte l'ultimo) non conosce contemporaneamente l'indirizzo del destinatario e il contenuto del messaggio, quindi abbiamo una buona sicurezza anche qualora parte della catena risultasse compromessa.

Ultimamente è anche in fase di realizzazione un **nuovo protocollo chiamato Type III** (che originalità!) associato al progetto **Mixminion**. Tuttavia questo protocollo non ha ancora raggiunto una forma stabile, cosa dimostrata anche dal fatto che parecchie nuove versioni di Mixminion (che dovrebbe essere un server/client Type III) non mantengono la compatibilità con le versioni precedenti. Proprio per questo motivo è difficile dare delle descrizioni precise del funzionamento del Type III (anche nel documento ufficiale che illustra il protocollo alcuni tratti sembrano abbastanza "nebbiosi"), ma se volete tenervi informati sullo sviluppo e se volete provare ad usare le versioni attuali di Mixminion, visitate il sito www.mixminion.net.

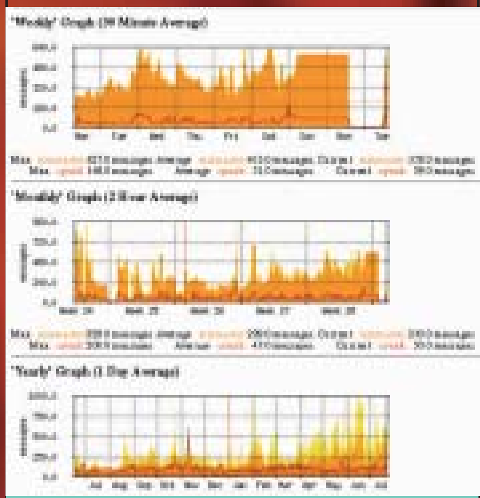
## >> Non sono tutte rose

Uno dei problemi principali nell'uso dei remailer anonimi, specie se usati in catena, **è la loro affidabilità**. Siccome un remailer anonimo può essere usato per **compiere azioni scorrette o addirittura illegali** (spam, ma anche minacce, ingiurie, diffamazione e scambio di materiale illecito), **capita abbastanza frequentemente che un remailer venga chiuso** per pressioni da parte della Giustizia, di una parte lesa, o più frequentemente da parte del provider che offre la connettività, che preferisce non avere grane. Al solito, per colpa di pochi che abusano di un servizio, molte persone che ne hanno davvero bisogno rischiano di rimanerne prive. Prima di usare un remailer, è bene quindi **verificare se ancora funziona**; molto spesso le liste dei remailer anonimi attivi che si trovano su Internet, mostrano anche delle statistiche di affidabilità, che è bene consultare.

Bene, queste sono le basi sufficienti per iniziare a inviare delle semplici mail anonime.

Vi consiglio di fare prima un po' di prove finché non siate completamente padroni del sistema.

**Piergiorgio Cardone a.k.a. gufino2**
**bugsman@libero.it**




Uno dei problemi dei remailer anonimi è la loro affidabilità. Per questo molti rendono disponibili anche delle statistiche sul loro stato. Qui sopra vedete una delle tante statistiche pubblicate da Autistici.org, all'indirizzo http://remailer.autistici.org/stats/

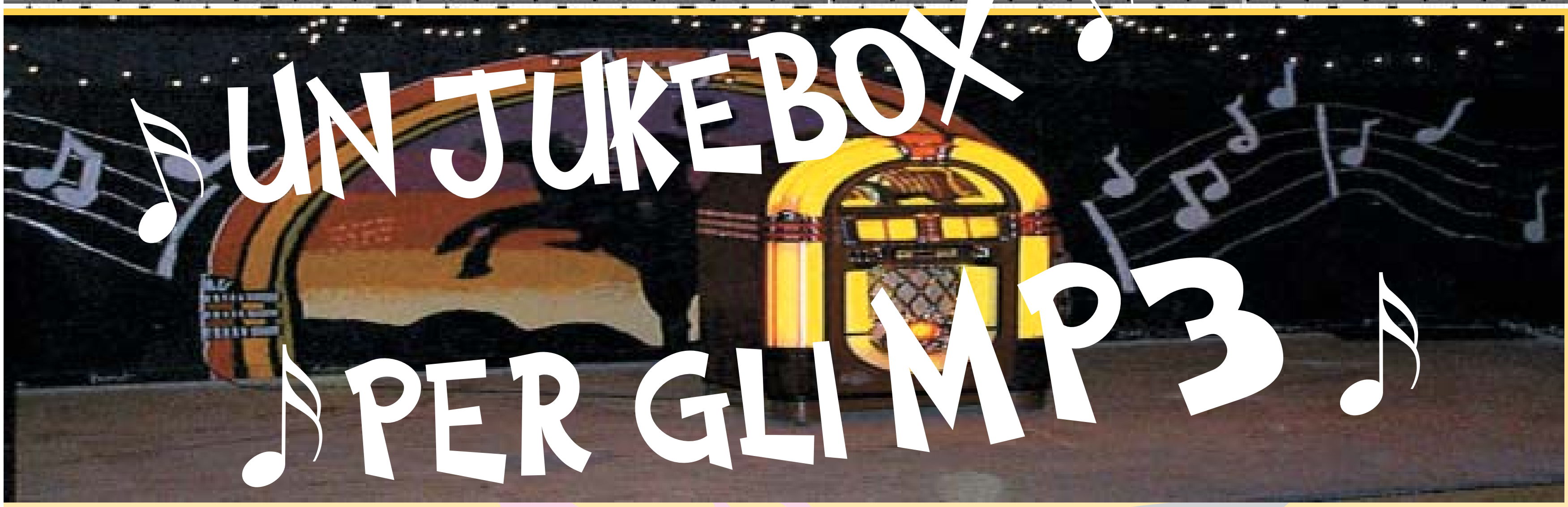
### LINK UTILI...

PGP Freeware 6.0.2
ftp://ftp.ch.pgpi.org/pub/pgp/6.0/6.0.2/PGPfreeware602.exe

Mixmaster
http://prdownloads.sourceforge.net/mixmaster/MIX204b46.zip?download

Jack B. Nimble
ftp://ftp.skuz.net/pub/potato/setup_jbn214.exe

Lista di remailer anonimi
http://anon.efga.org/Remailers



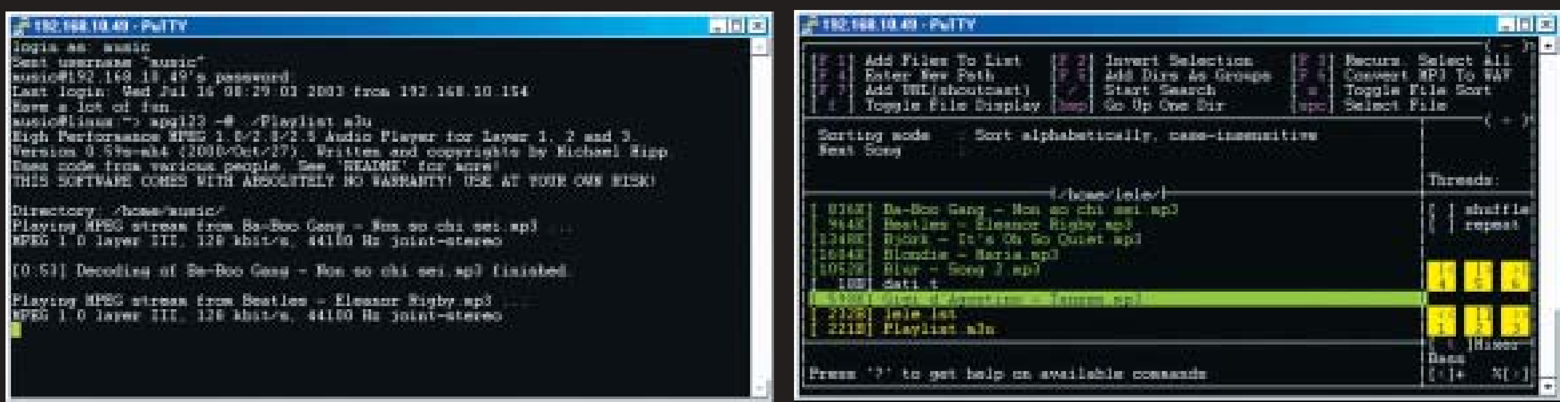
# UN JUKEBOX PER GLI MP3

**Un vecchio computer nascosto in un armadio e collegato allo stereo di casa può trasformarsi in un sistema per la riproduzione di musica.**

Siete davvero sicuri che quel vecchio PC, che da qualche tempo giace dentro l'armadio inutilizzato, non possa fare altro se non tenere compagnia a polvere e ragnatele? Per chi conosce Linux la risposta è scontata... Il nostro amato pinguino può esserci di grande aiuto anche in questo caso, riuscendo a **trasformare un computer oramai superati in un valido server Samba per reti eterogenee, in un router/firewall o in un server di posta**. Nulla vieta però di farne un utilizzo meno "tradizionale" ma non per questo meno divertente, creando **un vero e proprio jukebox Linux-based**! Immaginate il vostro vecchio PC sistemato in un angolo della stanza o nascosto nell'armadio e connesso allo stereo mentre voi, seduti sul divano con l'ultimo numero di HJ in una mano e il vostro palmare nell'altra, vi connettete via rete al Juke-Linux-Box e **lanciate la vostra compilation preferita**... Bello vero? Non perdiamo quindi altro tempo ed iniziamo subito a realizzare questo piccolo gioiellino...

## >> Cosa serve

Come premesso, non serve un computer molto potente (già un **Pentium 133 è sufficiente**) e nemmeno una quantità esagerata di RAM (**32 Mb andranno più che bene**); **una scheda audio degna di questo nome** è però consigliabile, così come un po' di **spazio libero sull'hard disk** ove poter conservare tutti gli MP3. Per quanta riguarda la distribuzione, potete tranquillamente utilizzare la vostra preferita, sia essa SuSE o Slackware o Mandrake; il consiglio è però quello di verificare prima di tutto se il vostro hardware (scheda audio in primis) è correttamente supportato. Considerato che non dovremo utilizzare l'interfaccia grafica, potrete **evitare direttamente di installare X, KDE, Gnome e vari Window Manager** e pacchetti annessi e connessi; inoltre è opportuno formattare le partizioni **utilizzando un journaled file system** (Reiser o Ext3 ad esempio), così da evitare intoppi in caso di riavvii indesiderati dovuti a sbalzi di tensione o simili cause.
Dovendo interamente gestire il nostro



Una volta connessi al jukebox, lanciate il vostro player preferito e.. alzate il volume!

## SUONARE CON LA TASTIERA

Il documento ufficiale di riferimento per la riproduzione e l'utilizzo di MP3 sotto Linux è senza dubbio l'MP3-HowTo del Linux Documentation Project (http://tldp.org/HOWTO/MP3-HOWTO.html). Per quanta riguarda in particolare i player MP3 per console, le alternative non mancano di certo e c'è solo l'imbarazzo della scelta. Di seguito ne presentiamo alcuni: a voi il compito di provarli e decidere a quale affidarvi...

**mpg123**
www.mpg123.de
Mpg123 è il più noto player audio disponibile per console Unix; oltre ad essere estremamente portabile, è persino in grado di funzionare, riducendo la qualità di riproduzione, su un 486. Sono inoltre stati scritti numerosi frontend che, appoggiandosi ad mpg123, permettono di creare e gestire playlist e quindi di riprodurle senza dover utilizzare esclusivamente la linea di comando; tra i tanti citiamo solo amf (http://amf.sourceforge.net/), gamp (www.cs.umn.edu/~wburdick/), jb (www.dtek.chalmers.se/~kw/jb/) e Juice (http://juicy.sourceforge.net/).

**mpg321**
http://mpg321.sourceforge.net
mpg321 è un clone completamente libero (rilasciato sotto licenza GPL) di mpg123 in grado di rimpiazzare egregiamente ed in maniera trasparente quest'ultimo.

**mp3blaster**
www.stack.nl/~brama/mp3blaster.html
Mp3blaster funziona interamente in modalità testuale e non necessita pertanto di un ambiente grafico quale X-Window; l'interfaccia di cui dispone permette tuttavia il player da tastiera in maniera estremamente intuitiva, come fosse un qualsiasi altro player dotato di GUI.

**linuxeyes**
:http://lug.orizont.net/~linuxeyes/
Come mp3blaster, anche questo player dispone di un'interfaccia grafica che ne semplifica l'utilizzo; merita sicuramente di essere provato, anche se non è open source ed è ottimizzato per il recente gcc3.

jukebox da remoto, occorrerà anche installare sulla macchina in questione gli appositi servizi, così da **permettere l'accesso via rete**. Tuttavia, sebbene il servizio Unix per l'accesso remoto tramite terminale sia storicamente Telnet, è preferibile non affidarsi a quest'ultimo, preferendo invece SSH. Infatti in una connessione Telnet i dati che il client passa al server e viceversa circolano in chiaro, senza venir cioè cifrati e non fornendo quindi alcuna protezione; **SSH (Secure SHell)** è nato proprio con lo scopo di garantire connessioni sicure a shell remote, implementando algoritmi a chiave asimmetrica (come quelli utilizzati ad esempio da PGP) per la cifratura dei dati. Insieme al servizio di remote shell sostitutivo di Telnet, SSH consente anche la **copia ed il trasferimento di files tra client e server con SCP e SFTP**. Ad esempio con SFTP potremo spostare sul nostro juke-Linux-box gli MP3 che poi andremo ad ascoltare, rimuovere quelli che non ci interessano più o persino scaricare in locale alcuni brani presenti su di esso, proprio come se fosse un vero server Ftp. Se l'idea vi alletta, provate quindi ad installare ed avviare sulla macchina il servizio sshd e.. stupitevi.



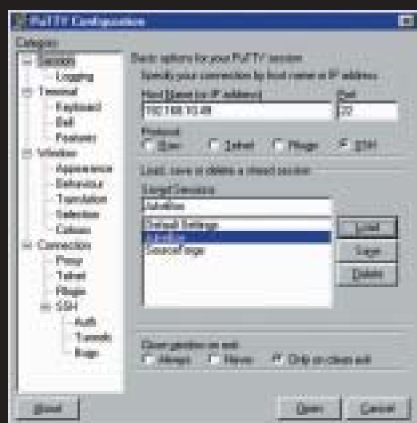

### >> Il riproduttore di MP3

Un discorso particolare merita il player: connettendovi al computer tramite shell testuale **non potrete infatti utilizzare i vostri amati player personalizzati** ad hoc con tanto di skin quali XMMS o Zinf (ex FreeAmp). Esistono tuttavia numerosi pacchetti appositamente scritti per permettere a tutti gli utenti di **utilizzare la shell nuda e cruda** senza dover per questo rinunciare ad un po' di buona musica; seppur diversi tra loro, sono tutti estremamente potenti e quindi poco importa che decidiate di utilizzare il classico **mpg123** o il suo clone libero **mpg321** o ancora l'accattivante **mp3blaster** piuttosto che **ogg123**.
Ricordate infine che utilizzare il sistema per le normali attività può rivelarsi estremamente dannoso per la vostra salute, nonché per quella del sistema! **Create pertanto un nuovo account** apposito sulla macchina (ad esempio 'music'), così da poter effettuare il login via ssh con questo utente ed **evitare di dover lavorare come amministratore**.
E' giunto quindi il momento di lasciar spazio alla fantasia; a voi ora il compito di costruire il vostro jukebox ed il dovere morale di inviarne una foto in redazione :)

**Lele**

## CONNESSIONI SICURE CON SSH

Tra le diverse implementazioni, commerciali o più o meno libere, del protocollo SSH che sono state scritte è sicuramente degno di nota l'ottimo pacchetto OpenSSH. Non solo infatti OpenSHH (http://openssh.org) è open source e disponibile per moltissimi Unix (tra cui ovviamente Linux), ma è strettamente connesso con il progetto OpenBSD, la distribuzione BSD con un occhio (forse anche due...) di riguardo proprio per gli aspetti legati alla sicurezza.
Il fatto che Unix/Linux (e quindi anche Mac OS X) supportino nativamente SSH non significa però che gli utenti Windows non possano instaurare connessioni remote sicure con un server utilizzando questo protocollo. In particolare il client più utilizzato per questo scopo è PuTTY (www.chiark.greenend.org.uk/~sgtatham/putty/), estremamente compatto e versatile nonché open source; inoltre dalla stessa home page del progetto è possibile scaricare gli altri tool del pacchetto SSH per la generazione di chiavi o per il trasferimento di file, utili proprio in un caso come quello del nostro jukebox con un cuore Linux. Sempre a tal proposito, gli amanti delle interfacce grafiche invece gradiranno sicuramente WinSCP (http://winscp.vse.cz/eng/), una versione user-friendly proprio dei tool di PuTTY per lo scambio di file via scp o sftp.





# PC Telefono Casa

## Le rete può rivelarsi una preziosa alleata per rintracciare i computer rubati: grazie a database e programmi spia. Scopriamo come.

Il furto di computer è una triste realtà con cui fare i conti quotidianamente. Negli Stati Uniti il fenomeno è diffuso e, a fronte di casi in cui il ladro viene effettivamente rintracciato e acciuffato, sono invece molti i computer persi per sempre.

Un tentativo per il ritrovamento di macchine "dubbie" è fornito da **alcuni archivi in rete, come "The Stolen Computer Database"** (www.amcoex.com/stolen/), **"Stolen Computers.org"** (www.stolencomputers.org/home.html) e, per i computer Apple rubati in Italia, il servizio Furti del Powerbook Owners Club (www.poc.it/stolen.html). Questi siti contengono elenchi consultabili dei numeri seriali di elaboratori sottratti e si indirizzano a chi vende e compra l'usato, per intercettare e, almeno in teoria, scoraggiare il furto e la ricettazione.

Inoltre, se per i computer desktop è ancora possibile usare lucchetti e cavi per ancorare fisicamente la macchina, **nel caso dei portatili, che nel 2002 hanno superato numericamente i sistemi desktop in quanto a numero di pezzi venduti, il problema è particolarmente grave.** I notebook vengono facilmente sottratti ed occultati durante viaggi, in sale d'aspetto di stazioni ed aeroporti ma anche in alberghi e ristoranti. A questo si aggiungono i numerosi casi di truffe, per esempio nelle compravendite per annunci o nelle ormai diffuse aste online.

Così negli ultimi anni si è registrato un fiorire di applicativi che assistono in vari modi l'utente ed ostacolano gli indesiderati. Anzitutto quelli che impediscono l'accesso fisico alla macchina richiedendo password, poi quelli che proteggono i dati nascondendo o cifrando il contenuto dei dischi fissi o delle partizioni.

Infine ci sono quelli, ed è su questi che ci concentreremo, che cercano di aiutare attivamente il proprietario a ritornare in possesso del proprio computer.

### >> Tatuaggi, come per i cani

Uno di questi è **Computer Watermark** (www.computerwatermark.com) per Windows, che fa uso del watermarking e cioè dell'**impressione invisibile di un marchio**, di un "sigillo". Questo metodo sarà sicuramente noto a chi si occupa di fotografia digitale,



Catene e lucchetti possono impedire il furto in un negozio o a una fiera, ma diventano inutili se il ladro si introduce in casa o in ufficio, e ha tutto il tempo di tagliarli o rimuoverli.

## QUALCOSA DI PIÙ ESTREMO

Partendo dall'assunto che la maggior parte dei ladri non può rubare ciò che non è in grado di trasportare, un eccentrico utente PC danese ha documentato e messo online (www.uoe.dk/csworld/security-.html) il suo personalissimo metodo per prevenire il furto del proprio computer. Il procedimento, degno più di un costruttore edile che di un informatico, è consistito sostanzialmente nel riempire il case di cemento fino all'orlo, raggiungendo il peso non indifferente di circa quaranta chili.
Anche se il computer è stato così reso completamente inutilizzabile, il risultato non indifferente è stato che per una intera settimana, seppur posto all'aperto, incustodito e in bella vista, il pc "sicuro" ha resistito al suo posto. Altrettanto incoraggiante è il bilancio di due mesi di "esposizione" in cui il case, seppur rimosso, non si è allontanato più di tanto, abbandonato in un fosso a un isolato di distanza, dopo aver presumibilmente provocato seri danni alla colonna vertebrale del ladro...

dato che diversi professionisti si tutelano così nel distribuire il proprio lavoro.
A detta dei produttori, Computer Watermark scrive nome e contatti del proprietario moltissime volte sullo spazio libero dell'hard disk. Se il PC dovesse essere controllato dalla polizia, o da un rivenditore o acquirente in buona fede, le scritte riveleranno la vera provenienza del computer. Purtroppo, il tutto si basa sulla presunzione che la polizia o l'acquirente conoscano questo tipo di "tatuaggio invisibile", e facciano la verifica.
Molto più numerose e diffuse, e sopratutto interessanti, sono però le soluzioni software accomunate dall'uso della strategia del "chiamare casa di nascosto".

## >> Se mi rubi, telefono a casa

La tecnica usata è sostanzialmente la stessa impiegata dai cosiddetti spyware, infausti programmi che, a insaputa dell'utilizzatore, di nascosto raccolgono dati su di noi e sul nostro computer e, alla prima connessione, spediscono il tutto ad un archivio centrale. Nel nostro caso però, i software vengono installati dal proprietario e sono a fin di bene in quanto mandano dei "segnali utili" a rintracciare il computer (per esempio un messaggio di posta elettronica). Alcuni lo fanno su base regolare, mentre altri solo se si accorgono che è cambiato qualcosa nelle configurazioni di rete.
È così che funzionano numerosi prodotti commerciali, shareware e freeware, come

**LapTrak**
(www.secure-it.com/products/asset_recovery.htm)
o **Absolute Protect**
(www.absolute-protect.com/), entrambi per Windows,
o **LapCop**
(http://homepage.mac.com/sweetcocoa/lapcop.html),
**Lost and Found X**
http://mirror.macupdate.com/info.php/id/8673)
e **Secure Notebook X**
(http://mirror.macupdate.com/info.php/id/8227) per Macintosh
o ancora **Stealth Signal Transmitter**
(www.computersecurity.com/stealth/)
e **PcPhonePro**
(www.pcphonehome.com/download.html), disponibili per entrambe le piattaforme.

Alcuni di questi programmi segnalano l'indirizzo IP del computer, oppure lo inviano, sempre di nascosto, ad un centro di raccolta del produttore del programma o addirittura possono impossessarsi della linea telefonica e chiamare numeri preimpostati (ad esempio quello di casa del lecito proprietario) permettendo così di identificare il chiamante (il ladro).

## >> Anche se il ladro formatta...

Una domanda però sorge spontanea: **e se il ladro rimuove o cancella tutto il contenuto del disco fisso del computer rubato?** Addio a ogni possibilità di risalire a lui e al computer?
Apparentemente è così, o meglio, si riteneva così fino alla fine di maggio di quest'anno, quando diverse testate informative online (http://news.com.com/2102-1046_3-1009807.html) hanno parlato della Softex, una ditta statunitense di Austin che ha annunciato una soluzione più radicale e meno facile da aggirare. **TheftGuard**, questo è il nome del prodotto, **è indipendente dal sistema operativo del computer e risiede nel BIOS della macchina**, per la precisione in quelli sviluppati dalla Phoenix, uno dei maggiori sviluppatori per PC compatibili x86.
Il programma si appoggia al "Core Managed Environment" della Phoenix e ogni volta che il calcolatore viene connesso ad Internet invia un "ping", un segnale al sito della ditta, dove il numero di serie verrà confrontato con quello delle macchine rubate. In caso affermativo si potrà non solo, come con gli altri programmi, rintracciare l'IP ma addirittura procedere a disabilitare alcune funzioni del PC o cancellarne i dati.

## >> Recuperare: ma a che costo?

Non possiamo fare a meno, però, di notare che sistemi come TheftGuard, che sono legati all'hardware e che promettono di resistere a tentativi di rimozione e di anonimizzazione del computer, suscitano qualche (legittimo) dubbio per il **potenziale abuso** che può esserne fatto.
L'inserimento "a monte" di sistemi atti al **rintracciamento e al controllo dei computer** riecheggia vicende passate come il caso del "clipper chip" o i rischi concreti dell'indirizzo MAC (Media Access Control), univoco e presente su ogni scheda di rete e che alcuni programmi poco "simpatici" come Word, possono trasmettere in documenti di testo all'apparenza banali.
Attenzione quindi ad affidarsi ciecamente a prodotti che promettono mari e monti ma che potrebbero sottrarci anche quel poco di privacy che resta...

Nicola D'Agostino
dagostino@nezmar.com




I software come LapTrak inviano periodicamente un segnale a un centro di controllo; se il computer risulta rubato, il segnale viene usato per individuare l'attuale proprietario (il ladro stesso, o qualcuno che lo ha acquistato da lui).

# NASCONDI I

## Sei programmi gratuiti per tenere i propri file lontani da

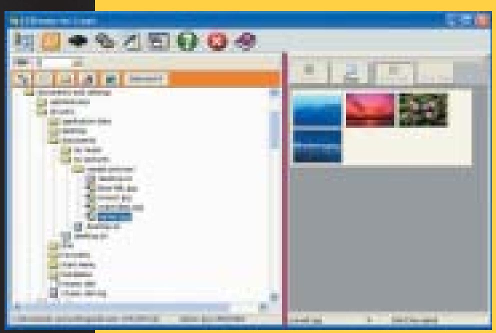
Al giorno d'oggi si cerca di ottenere sempre una maggiore sicurezza nei sistemi informatici e su Internet, a scapito della privacy degli utenti che si vedono spiati in quello che hanno sul PC e fanno su Internet. Spesso **è necessario tenere i propri file "sensibili" lontano da occhi indiscreti** o semplicemente nascondere dei documenti riservati a chi condivide l'uso dello stesso computer (colleghi, amici, famigliari).
In generale, quando bisogna nascondere dei file, esistono due strade: **renderli "invisibili"** o **cifrarli** in modo da renderli comunque illeggibili. In questa direzione si sono concentrati molti produttori di software per assicurare agli utenti una protezione dei loro dati e file. Le soluzioni offerte sono tantissime, si va dai programmi freeware che semplicemente nascondono una cartella, fino alla più elaborata cifratura dei propri dati con sofisticati programmi di crittografia. In quest'articolo parleremo di come poter nascondere in modo più o meno efficace i propri file e quali software usare a tale scopo.

### >> Ferri del mestiere

Prima di tutto bisogna ricercare un software di questo tipo a seconda delle esigenze dell'utente: nel caso di un utente privato che deve semplicemente nascondere una cartella o dei file sul proprio PC, sul web ci sono tantissimi software utilizzabili gratuitamente che rendono invisibili i file desiderati e accessibili solo tramite una password. In generale con un programma di questo tipo basterà selezionare il file tiziano-il-pallino.mpg da nascondere, scegliere la directory in cui operare, una password di accesso e il gioco è fatto! Per rendere di nuovo visibili le cartelle nascoste basterà attuare il procedimento inverso inserendo la password assegnata in precedenza. I punti di forza di questi metodi artigianali sono la semplicità, la velocità di utilizzo e il fatto che le cartelle nascoste risultano invisibili anche riavviando il sistema in modalità provvisoria o sotto Ms-Dos. Inutile dire che questo è il

## ZERO FOOTPRINT CRYPT 2.1

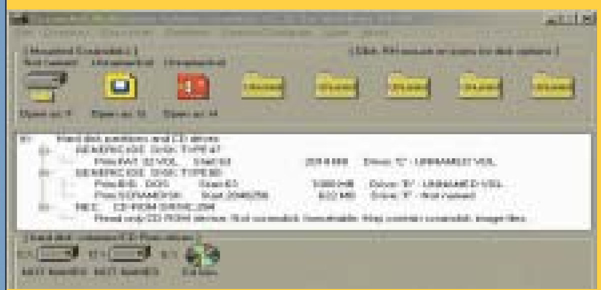
Sito: http://users.hol.gr/~kabriel/zerofootprint1.htm



In un mondo popolato da programmi fotocopia, ecco qualcosa di originale, ben pensato e soprattutto gratuito. Zero Footprint Crypt ha come obiettivo principale quello di non lasciare tracce sul disco (footprint, appunto). Per fare ciò, può cancellare in modo sicuro i file dopo averli cifrati, e riduce al minimo la necessità di decifrarli per l'utilizzo. Attraverso un modulo visualizzatore di file interno al programma stesso, è possibile vedere immagini o video leggendoli direttamente dal file cifrato, senza la necessità di registrarli prima in chiaro sul disco fisso. Geniale.
L'algoritmo usato (blowfish) è sufficientemente robusto per mettere in crisi anche i servizi segreti. Decisamente una scelta consigliabile.

## SCRAMDISK

Sito: www.scramdisk.clara.net



Parlando di altri sistemi operativi senza però toccare Linux, è altamente consigliato a tutti gli utenti di Windows 9x un software freeware di nome Scram Disk, che permette la cifratura automatica dei

NEWBIE

# TUOI FILE!

## occhi indiscreti, perché... “sono solo fatti miei”.

modo più elementare di proteggere i propri dati **e funzionerà solo con un incompetente** che sa appena accendere il PC. Altro accorgimento che è necessario prendere è quello **di non nascondere le directory “sbagliate”** che potrebbero compromettere il funzionamento del computer come C:\, C:\Windows, C:\Windows\System, C:\Programmi e via dicendo. La cosa migliore da fare è quella di salvare tutti i propri dati ‘sensibili’ all’interno di un’unica directory, che può contenere anche altre sottodirectory, e proteggere solo quella con un programma che la renda invisibile. Generalmente un mediocre programma di protezione freeware, facilmente scaricabile da Internet, è capace di offrire una soddisfacente protezione.

### >> Qualcosa di più sicuro

Per una protezione più avanzata e una maggiore sicurezza anche quando i dati ‘sensibili’ vengono scambiati su Internet, ci sono software più elaborati e programmi di crittografia a prova di bomba sviluppati apposta per le aziende che non possono permettere che qualcuno scopra i loro segreti. **Primo tra tutti è il classico programma di crittografia PGP** di cui abbiamo parlato nel numero 25, il quale cifra i nostri dati in modo da rendere quasi impossibile l’accesso a persone non autorizzate. Di crittografia si è già parlato spesso sulla nostra rivista quindi evito di entrare nei particolari dato che nei numeri precedenti trovate articoli molto dettagliati sui metodi utilizzati e i migliori software in questo campo.

### >> Occhio ai dettagli

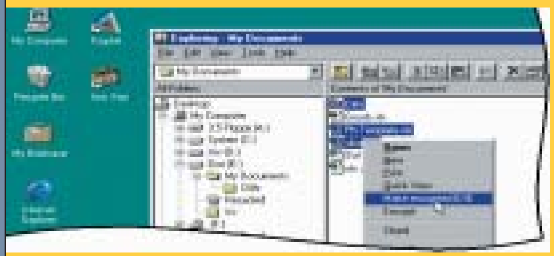
Un errore fatto da molti novellini è quello di nascondere o cifrare un file, ma di **lasciarne traccia in vari punti del disco fisso**, per esempio spostando il file originale nel Cestino e lasciandolo lì, o cancellarlo semplicemente svuotando il Cestino di Windows. Per eliminare completamente le tracce di un documento le normali fun-



file. L’ultima versione di ScramDisk per 9x è gratis ma potrebbe risultare un po’ vecchia perché non verrà più supportata e lascerà completamente il suo posto al suo successore DriveCrypt per Windows NT/XP, purtroppo a pagamento. Questa nuova versione costa ben 40 dollari, se si pensa che la precedente costava la metà, ma promette di offrire ottimi risultati agli utenti che ne rimarranno soddisfatti. In alternativa c’è BestCrypt, di cui è stata recentemente rilasciata una nuova versione, che costa di più (costa ben 89 dollari solo la versione 6, ormai superata dall’ultima uscita), ma mette a disposizione dell’utente caratteristiche uniche nel suo genere, come la possibilità di criptare lo swap file, un’originale protezione con doppia password (di cui una è falsa).

### IRON KEY

Sito: www.kryptel.com/products/ikey



Iron key è in grado di trasformare qualsiasi file in un file .exe protetto da password. Ovviamente chi ha accesso al nostro computer ed è interessato a quel file sarà in grado di trovarlo senza problemi, ma non potrà avere accesso ad esso: per decodificare il file occorre inserire, quando richiesta, la password giusta. Utilizzarlo è semplice: cliccando col tasto destro sul file da proteggere si potrà scegliere di codificare il file e se cancellare i file originale; inserita la password, si avrà un file exe protetto. Tra i tanti punti deboli di Iron Key ci sono le limitazione di questa versione gratuita: non cripta un insieme di file ma soltanto un file per volta e non è in grado di criptare le cartelle.

zioni di cancellazione di file del sistema operativo non bastano: per essere sicuri che il file non possa essere recuperato con programmi che ripristinano i documenti cancellati, bisognerà usare un'utility che cancelli il file in modo definitivo, sovrascrivendolo varie volte con dati casuali.
A volte, **il semplice nome del file può rivelare ciò che si voleva tenere nascosto**: un capo ufficio che, nei menu dei file aperti di recente trova documenti con nome **Supertettona.mpg** o **Curriculum.rtf** non ha bisogno di vedere il contenuto del file per capire che l'impiegato sta usando il computer per scopi non propriamente lavorativi nel primo caso, o sta cercando di cambiare lavoro nel secondo.

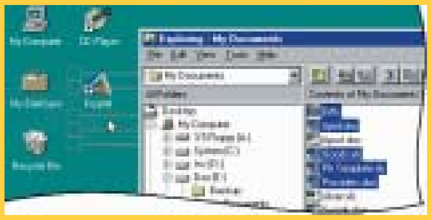
{RoSwEIL}

## SU MACINTOSH...



Chi utilizza Mac OS X può creare volumi cifrati usando l'applicazione Disk Copy, che fa parte del sistema operativo (la si trova in Applcazioni/Utility). Disk Copy può essere usata per aprire o creare immagini disco, che si presentano come file con estensione .dmg ma –una volta aperte– sono disponibili sulla Scrivania come se fossero dischi rimovibili. Quando si crea una nuova immagine disco, si può selezionare nell'opzione Criptatura l'algoritmo AES-128.

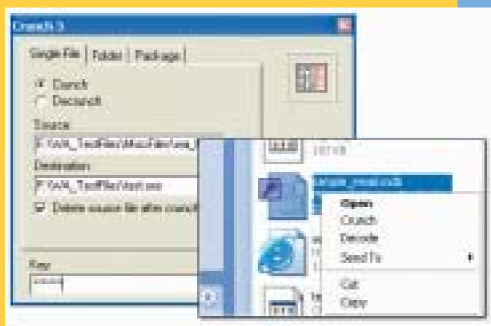
## KRYPTEL LIGHT



Sito: www.kryptel.com/products/krlite/

Dallo stesso produttore di Iron Key, Kryptel Light è la versione ridotta e gratuita di un programma commerciale più tradizionale. Il file viene cifrato con l'algoritmo DES, e può essere anche immediatamente cancellato in modo sicuro. Kryptel Light si integra nel sistema operativo, permettendo di cifrare file usando il solo tasto destro del mouse, oppure trascinandoli sull'icona del programma. Può anche integrarsi con altri programmi della stessa azienda, come lo stesso Iron Key, per aumentarne la sicurezza.

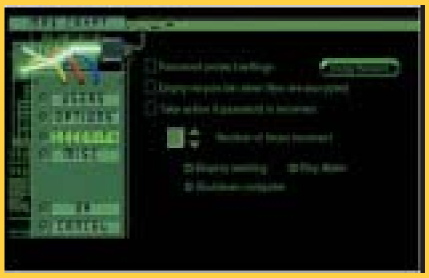
## CRUNCH



Sito: http://software.iamcal.com

Punto di forza di Crunch è probabilmente la praticità: può lavorare su singoli file o intere cartelle. Le cartelle possono essere racchiuse in un singolo file, o cifrate in una nuova sotto cartella. Ogni volta che si cifra un file, è necessario inserire una password, che potrà quindi essere diversa per ciascun file (occhio a ricordarsele però…). I file possono essere cifrati trascinandoli nell'interfaccia di Crunch, o con una semplice pressione del tasto destro del mouse.

## MAXCRYPT



Sito: www.kinocode.com/maxcrypt.htm

Il bello di MaxCrypt è che lavora in modo trasparente: singoli file, cartelle o interi dischi vengono cifrati quando si spegne il computer, e decifrati quando si lancia il programma (magari in automatico all'avvio del computer). In questo modo i file sono sempre accessibili quando il legittimo utente sta lavorando al computer, ma non possono essere letti da un altro utente o da qualcuno che si rubi l'hard disk o l'intero computer.

## RIPCODER



Sito: http://kach.nm.ru/

L'interfaccia non è delle più amichevoli, e anche le opzioni da impostare non sono semplicissime. Se questo non vi fa paura, Ripcoder è un programma molto potente, che usa algoritmi di cifratura molto robusti, come 1st, Blowfish, TripleDES e DES+. L'ultimo, in particolare, è praticamente inattaccabile se il file da cifrare è molto grande (e la password scelta non è ovvia). L'uso è gratuito, ma se si effettua una donazione, si riceve la documentazione completa, e una particolare dll personalizzata, senza la quale i file non possono essere aperti, neanche con la password.

# PROTOCOLLO IP+SECURE=IPSEC

## Il metodo più promettente per ottenere comunicazioni sicure, cifrate, non intercettabili e non spoofabili su protocollo IP.

Nel numero scorso di HJ abbiamo trattato l'argomento VPN con una panoramica sulla loro struttura e sul concetto generale di tunneling ip, con la descrizione di alcuni protocolli. Questo articolo sarà dedicato esclusivamente al **protocollo IPSec, considerato al momento il migliore in circolazione per il tunneling ip**, adottato da Microsoft su Windows 2000 e 2003 e implementato spesso dai sistemisti Unix. È opportuna a questo punto una precisazione: parlare di protocollo IPSec non è proprio corretto, giacché l'IPSec è uno standard costituito non soltanto da protocolli ma anche da altre parti. Dal momento che in ogni caso noi parleremo esclusivamente dei protocolli, mi si conceda questa 'licenza poetica'.

Come parecchi altri protocolli che l'hanno preceduto, anche l'IPSec si basa su **alcuni RFC** (di cui diamo un breve elenco nel riquadro) che sono in fase di ratifica da parte dell'IETF. Sono stati progettati per fornire dei servizi di protezione per il protocollo Ipv4 attualmente in uso e per il futuro Ipv6.

IpSec è costituito da due differenti protocolli utilizzati per offrire **due diversi livelli di protezione**: stiamo parlando dell'**IP Authentication Header** (AH) e dell'**IP Encapsulating Security Payload** (ESP per gli amici). Vediamo in dettaglio il funzionamento di entrambi.

### >> IP Authentication Header

L'IP Authentication Header, che chiameremo da ora in poi AH, è definito nell'**RFC 2402** e fornisce servizi di autenticazione, impossibilità di risposta e l'integrità per l'intero pacchetto, ma non effettua la crittografia dei dati. Vediamo di capire meglio cosa significano questi paroloni…

• Il servizio di **Autenticazione** fornisce una serie di metodi di autenticazione, tra cui per esempio l'autenticazione Kerberos (ne abbiamo già parlato più volte su HJ).

• Per **"impossibilità di risposta"** si intende l'impossibilità da parte di un terzo, estraneo ad una comunicazione, di intercettare i dati e riutilizzarli senza necessariamente riuscire a decifrarne il contenuto, come potrebbe succedere nel caso in cui si intercettassero i dati di autenticazione anche se cifrati. Un esempio tipico di una pratica di questo tipo è il riutilizzo degli hash di LanManager su Windows NT. IpSec impedisce tutto ciò con una tecnica chiamata CBC (Cipher Block Chaining) che rende unico ogni pacchetto generato anche se il contenuto dei dati è il medesimo.

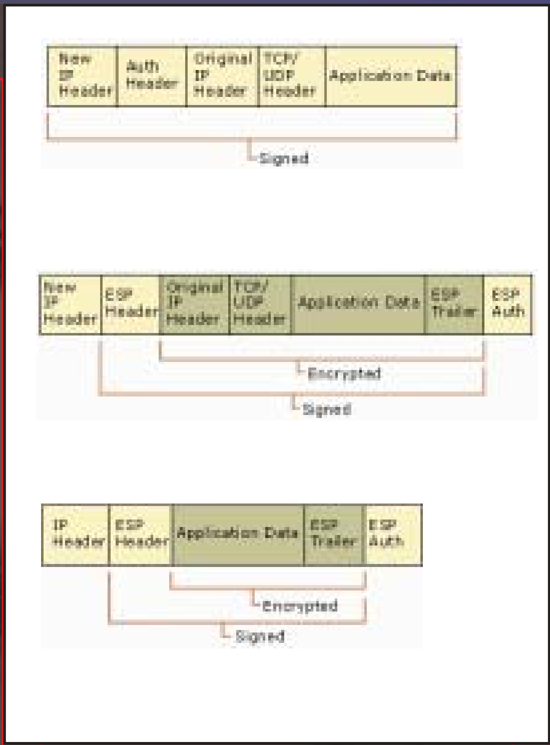
• Per **"integrità dell'intero pacchetto"** si intende l'impossibilità da parte di un terzo di modificare i pacchetti in transito, poiché i pacchetti vengono tutti contrassegnati da una firma digitale ottenuta con algoritmi del tipo di MD5 (Message Digest 5) e SHA1 (Secure Hash Algorithm 1), attraverso una chiave condivisa dai due sistemi in comunicazione. Questa sorta di firma digitale sui pacchetti viene chiamata MIC (Message Integrity Code).

L'applicazione di questi servizi da soli però **non impedisce la semplice intercettazione e lettura,** dal momento che i dati veri e propri non vengono cifrati. A questo punto qualcuno potrebbe chiedersi: che fine ha fatto allora l'impossibilità della risposta? L'im-

possibilità della risposta riguarda esclusivamente il riutilizzo di pacchetti così come sono in un momento diverso da quello in cui sono stati generati, questo indipendentemente dai dati contenuti.
Quindi in fin dei conti le garanzie che può darvi AH sono che i dati arriveranno al destinatario, che non verranno dirottati, che i pacchetti non saranno riutilizzati o modificati.

## >> Come opera AH sui pacchetti

Il protocollo AH aggiunge **un'altra intestazione al datagramma IP**. Tale intestazione viene inserita tra l'intestazione IP del pacchetto e le intestazioni successive, cioè quelle del protocollo del livello di trasferimento (TCP, UDP, ICMP). Se il pacchetto contiene altri protocolli (come per esempio ESP, che vedremo subito dopo), le relative intestazioni vengono inserite immediatamente dopo l'intestazione AH.
L'intestazione AH ha la struttura indicata nello schema in figura. Il primo campo di 8 bit indica il tipo dell'**intestazione successiva**. Generalmente troviamo i valori 6 o 17 che indicano rispettivamente intestazioni TCP e UDP. Se sul pacchetto è stato applicato anche ESP, la sua intestazione, che come abbiamo detto si andrà a inserire subito dopo quella di AH, verrà preannunciata nell'intestazione AH con la presenza del valore 50 nel campo **intestazione successiva**.
Il secondo campo è sempre di 8 bit ed indica semplicemente la **lunghezza dell'intestazione** AH. Poi vi è un terzo campo di 16 bit destinato a utilizzi futuri.
Il quarto campo di 32 bit ha un importanza fondamentale perché è **l'indice dei parametri di protezione**. Qui è contenuto un valore arbitrario che identifica un'**associazione di protezione (SA)**. L'associazione di protezione è un accordo tra due computer sulle misure di protezione utilizzate durante la trasmissione.
Nel quinto campo di 32 bit è contenuto il **numero di sequenza**. Quest'ultimo, insieme al campo precedente, fornisce quel servizio di impossibilità di risposta di cui abbiamo parlato in precedenza. L'accoppiata **associazione di protezione** e **numero di sequenza** è infatti unica per ogni pacchetto. Se il computer ricevente verifica di aver già ricevuto un pacchetto con un certo numero di sequenza e un certo SA, lo rifiuta.
Infine, troviamo i **dati di autenticazione**. Questo campo contiene l'ICV (Integrity Check Value) che viene calcolato su tutte le intestazioni, sia quella IP precedente, che quelle successive alla AH ed i dati contenuti. Questo per evitare che il pacchetto possa essere parzialmente modificato durante il transito.




## >> IP Encapsulating Security Payload (ESP)

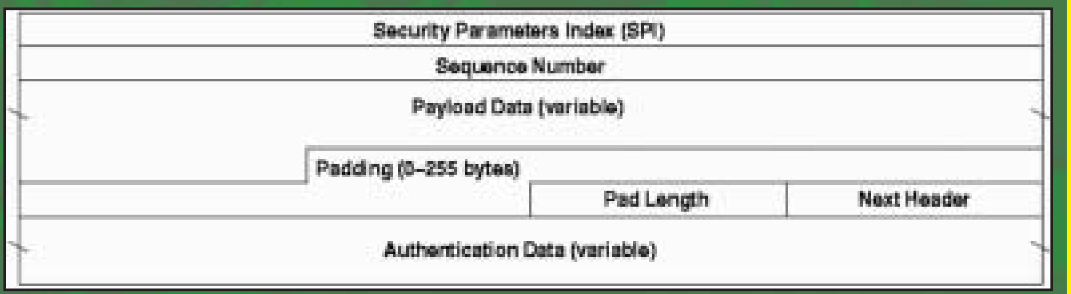
Il protocollo IP ESP dello standard IPSec fornisce servizi di crittografia dei dati contenuti nei pacchetti, **integrità** e **impossibilità di risposta**. La differenza fondamentale tra il funzionamento di AH e di ESP è che quest'ultimo non si limita soltanto ad aggiungere un'intestazione al pacchetto, ma **incapsula i dati nella sua struttura**. Tutti i dati che si trovano tra l'intestazione ESP e la pagina di riepilogo ESP (ESP trailer in figura) vengono cifrati. Un'ulteriore differenza con il protocollo AH è che l'ESP non include nel calcolo della firma digitale l'intestazione IP, quindi è possibile da parte di un terzo modificarlo e, per esempio, dirottare la sessione. Conviene quindi utilizzarlo insieme al protocollo AH per una maggiore sicurezza. Vediamo adesso nel dettaglio da quali campi è costituito un pacchetto ESP.
Abbiamo innanzitutto **l'indice dei parametri di protezione** di 32 bit che ha lo stesso ruolo del campo analogo dell'intestazione AH: cioè qui è contenuto un valore arbitrario che identifica l'accordo SA tra i due sistemi in comunicazione. Il secondo campo è il numero di sequenza, 32 bit. Questo è il campo che fornisce il servizio di **impossibilità di risposta** (anti spoofing). Il funzionamento è uguale a quanto descritto per l'AH.
Campo caratteristico del pacchetto ESP è il campo **dati payload**, di lunghezza variabile, in cui è stato incapsulato e crittografato il pacchetto originale completo di intestazione e dati applicazione.
Il campo di **spaziatura interna** (padding) varia da 0 a 255 byte e viene utilizzato per allineare i due campi successivi in una parola a 32 bit: ciò perché il campo precedente ha una lunghezza variabile. Questo allinea-

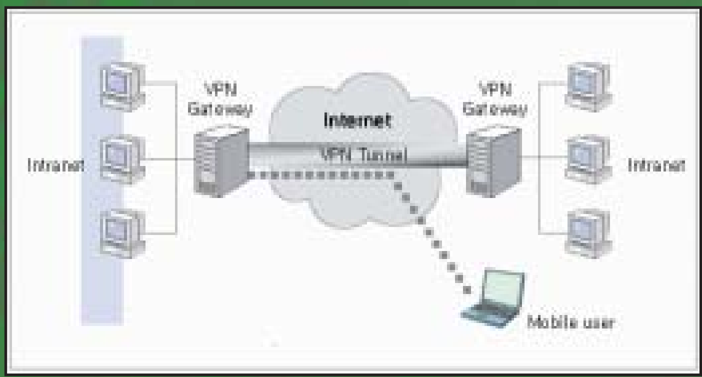
### I DOCUMENTI PRINCIPALI

Ecco i più importanti RFC che riguardano IPSec. Li trovate sui siti che raccolgono le RFC, come per esempio: www.rfc-editor.org

- RFC 2411 IP Security Document Roadmap
- RFC 2401 Security Architecture for the Internet Protocol
- RFC 2402 IP Authentication Header
- RFC 2403 the use of HMAC.MD5-96 within ESP and AH
- RFC 2404 the use of HMAC-AHA-1-96 within ESP and AH
- RFC 2406 IP Encapsulating Security Payload (ESP)




mento è necessario per alcuni algoritmi crittografici che lavorano con blocchi di dati aventi una lunghezza specifica, inoltre fa in modo che il campo successivo, contenente i dati di autenticazione, possa cominciare da un limite di 32 bit. Il campo **lunghezza pad** di 8 bit contiene un valore che indica il numero di spazi di cui è costituito il campo di spaziatura interna. Il campo **intestazione successiva** di 8 bit contiene un valore convenzionale che sta ad indicare l'intestazione immediatamente seguente l'intestazione ESP. Infine l'ultimo campo del pacchetto ESP riguarda i dati di autenticazione. Anche questo è un campo variabile e contiene l'ICV calcolato questa volta non su tutto il pacchetto, come avviene per AH, ma sulla parte compresa tra l'intestazione ESP e la pagina di riepilogo ESP. Questo campo serve per garantire l'integrità del pacchetto in transito.




## >> In una rete privata virtuale

Fino a questo momento abbiamo visto il funzionamento dei due protocolli di IPSec in modalità trasporto, cioè una modalità in cui l'intestazione IP del pacchetto originale non viene modificata.
Quando si implementa IPSec in una VPN però **è probabile che si disponga anche di gateway VPN,** come quelli visti nell'articolo sullo scorso numero di HJ. In questo caso è possibile utilizzare un'ulteriore modalità ancora più sicura: la modalità **tunnel** nella quale viene creata una nuova intestazione IP e tutto il pacchetto originale viene incapsulato tra l'intestazione ESP e la pagina di riepilogo che va a chiudere la parte ESP del pacchetto. Per questo motivo **è l'intero pacchetto ad essere crittografato,** e inoltre il protocollo AH genera un ICV calcolato sull'intero pacchetto.
In questo caso non è necessario che il sistema ricevente e quello trasmittente supportino IPSec, dal momento che **sono i gateway stessi ad effettuare la conversione da pacchetto normale a pacchetto AH-ESP** in modalità tunnel. Quando poi il pacchetto arriverà a destinazione, troverà dall'altra parte un gateway che sarà in grado di riconvertire il pacchetto in un normale pacchetto IP leggibile da qualunque sistema che supporti TCP/IP.

**Roberto 'decOder' Enea**

# LINK UTILI

www.ietf.org/html.charters/ipsec-charter.html
Sito del gruppo di lavoro dell'IETF su IPSec

www.netbsd.org/Documentation/network/ipsec/
Interessante faq su VPN e IPSec

http://sourceforge.net/projects/ipsec-tools
Per chi si volesse cimentare ecco il sito del progetto ipsec-tools su sourceforge.net

# File system Journaled su Mac



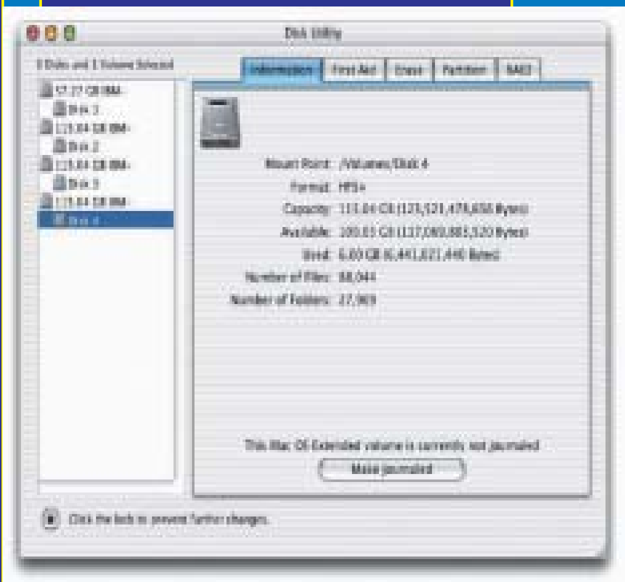
**Journaling: un diario di sicurezza per il disco fisso. Scopriamo la recente funzione del filesystem di OSX, pensata per i server, ma interessante anche per l'utente comune.**

Dalla versione 10.2.2 MacOS X ha visto l'introduzione ufficiale di una funzione di journaling per i dischi e le partizioni nel formato HFS+ (Extended Mac OS, in Italia Mac OS Esteso).
Il journaling (nome in codice "Elvis") è una funzione già disponibile su alcuni sistemi operativi come **Linux**, **OS/2** e lo sfortunato **BeOS,** ed è un sistema con cui il computer mantiene un log, o un "journal" (da cui il nome) cioè **"tiene traccia" di tutte le operazioni che compie sul disco fisso**. Lo scopo è quello di **facilitare il ripristino dei dati**, ad esempio dopo un crash o dopo un' interruzione di corrente. Con un filesystem di tipo "journaled" è molto facile quindi **riportare la macchina allo stato in cui era prima del malfunzionamento** senza la necessità di usare (ed aspettare l'esito di) strumenti per controllare e riparare problemi alla struttura software dei dischi.
Apple ha introdotto e raccomanda (e fornisce l'assistenza) del journaling sulle **versioni Server di OSX** e più avanti vedremo anche come gestire questa funzionalità. Il journaling viene consigliato come misura addizionale (possibilmente in congiunzione a un sistema di dischi RAID ridondante, gruppi di continuità e frequenti backup) su macchine server che hanno esigenze e caratteristiche particolari. Queste inoltre sono meglio attrezzate come hardware e software (più RAM, dischi più veloci e con cache ottimizzate) a **sopportare lo stress maggiorato che il journaling impone all'hard disk e al processore**.
Ciò non vuol dire che non sia possibile farne uso anche sulle "semplici" macchine con la versione client di OSX, anzi. A patto di avere montata **parecchia RAM** (pena l'entrata in conflitto con la funzione di memoria virtuale) e di **accettare una lieve diminuzione delle prestazioni generali**, anche le macchine "casalinghe" possono trarre giovamento da un livello di sicurezza e tranquillità maggiori che il journaling offre. È il caso ad esempio di **chi ha un portatile** ed espelle per errore la batteria mentre non è collegato all'alimentazione, **o abita in una zona suscettibile a black-out** o ancora si **"dimentica" di smontare share SMB**.

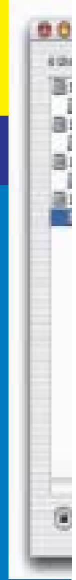


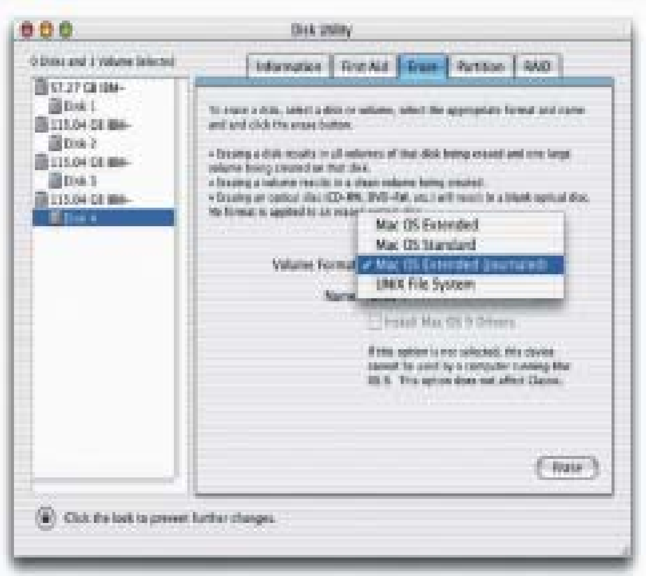
## >> Filesystems journaled: verso il futuro

Il journaling fa in realtà parte di una serie di miglioramenti incrementali delle caratteristiche del filesystem HFS+ (nome in codice "Sequoia") del Mac OS e, garantendo la piena compatibilità all'indietro, si inquadra in una precisa strategia tecnologica della Apple. Questa si basa sul concetto di **trattare l'intero filesystem come un database** ed è comune all'implementazione



del journaling in altre piattaforme, come l'Ext3 di Linux, il JFS di HP-UX, AIX e OS/2 5 e sopratutto il BeFS, il filesystem del BeOS. Chi ha avuto modo di provare lo sfortunato sistema fondato dall'ex capo ingegnere Apple Jean Louis Gasseé, forse avrà notato che **in BeOS la gestione, la ricerca e il reperimento di documenti di vari tipi sono efficaci e rapidi** perché il sistema in realtà organizza il contenuto dell'hard disk sotto forma di base di dati, interrogabile in qualsiasi momento secondo criteri definiti dall'utente.
Un concetto molto valido, tant'è che qualcosa del genere è in preparazione anche a Redmond: **il prossimo**






**Windows, chiamato Longhorn, avrà un filesystem di questo tipo**, basato sul database Microsoft SQL.

Ma la Apple non sta a guardare e **ha assunto Dominic Giampaolo, autore del filesystem del BeOS**, ora al lavoro sul prossimo MacOS X, nome in codice Panther.

## >> Attivazione e disattivazione

Il journaling può essere implementato **senza bisogno di formattare il disco rigido**, a patto che **questo sia in formato HFS+ (e non HFS o UFS). Allo stesso modo non è necessario intraprendere complicate installazioni o aggiornamenti del sistema operativo**: in OSX Server è disponibile una comoda interfaccia grafica per la gestione del Journaling.
E' sufficiente usare il programma della Apple per la gestione di dischi (allegato in ogni installazione di sistema) "**Disk Utility**" e selezionare (nella versione inglese) il pulsante in basso "**Make journaled**". Nel caso che il disco o la partizione non siano nel formato giusto, nel terzo tab in alto, dal titolo "Erase" si può provvedere a **riformattare e scegliere da subito un formato journaled**.
Se invece non ci si trova sulla versione Server, possiamo usare il già citato tool multiuso **Cocktail** (www2.dicom.se/cocktail), che, tra le ultime funzioni, ha implementato anche l'attivazione (e disattivazione) del journaling. Come al solito in OSX è possibile usare anche metodi più diretti e tipici di UNIX. Il journaling infatti è **attivabile anche da linea di comando** e può essere gestito anche in remoto tramite un collegamento SSH (Secure Shell).
Il programma nella shell che fa al caso nostro è "**diskutil**". Digitando nel Terminale:

```
/usr/sbin/diskutil
```

ci apparirà la schermata informativa del Disk Utility Tool con i comandi e le varie opzioni, tra cui

```
diskutil info /percorsodeldiscoo
                partizionescelta
```

che ci fornisce informazioni su dischi e partizioni ma sopratutto le due opzioni:

```
enableJournal      (Enable   HFS+
    journaling on a mounted HFS+
                         volume)
disableJournal    (Disable   HFS+
    journaling on a mounted HFS+
                         volume)
```

Per abilitare il journaling bisogna digitare

```
sudo  diskutil  enableJournal  /
percorsodeldiscoopartizionescel-
ta
```

Un esempio di attivazione sul disco principale può essere:

```
[nezmars-Computer:~] nezmar%
sudo diskutil enableJournal /
```

Una volta dato invio e fornita la password di amministratore, il computer si metterà al lavoro per qualche istante e, seguito da alcune informazioni sullo spazio occupato, genererà il messaggio di conferma:

```
Journaling has been enabled on /
```

Per disattivare, nulla di più semplice che digitare:

```
sudo diskutil disableJournal /
```

Nel caso di un crash, il sistema al riavvio comunicherà di aver fatto **un "replay" del journal**, cioé di essere tornato indietro nel log, il diario delle azioni, che l'OS tiene del disco. Questo **non vuol dire che l'integrità del filesystem sia garantita sempre e comunque**. In alcuni rari casi può essere comunque necessario riavviare in single-user mode e usare utility di terze parti, o impostare da Terminale il comando

```
fsck_hfs -f /dev/nomedeldisco
```

## >> Considerazioni sull'uso.

Come già detto il journaling **ha un costo in termini di prestazioni**. Quantificare questo costo è difficile in quanto dipende da una serie di fattori: **alcune fonti parlano di un rallentamento fino al 20%** nel caso di MacOS X client.
Altre fonti parlano di un calo di performance nullo o comunque trascurabile, **intorno al 5%**, sopratutto in presenza di forti quantità di memoria RAM (un giga circa), il che previene sopratutto l'uso della memoria virtuale, un'opzione meno che ottimale in quanto questa si "litiga" l'accesso al disco con il journaling. In ultima analisi la valutazione è soggettiva: per qualcuno i vantaggi possono valere il "performance hit", mentre per altri, più attenti in fatto di backup, una macchina meno reattiva è inaccettabile. A questo punto non resta che provare ad attivare il journaling e valutare pro e contro, sul campo, nell'uso quotidiano.

**Nicola D'Agostino**
**dagostino@nezmar.com**

## PER APPROFONDIMENTI:

Ecco un paio di siti da consultare subito. Altri link, troppo lunghi per essere pubblicati su carta, li trovate nella sezione Contenuti Extra dal sito di Hacker Journal.

**Filesystems-HOWTO**
http://penguin.cz/~mhi/fs/

**Mac OS X Server Technologies - File System Journaling**
http://www.apple.com/server/macosx/pdfs/L24481A_Journaling_TB.pdf

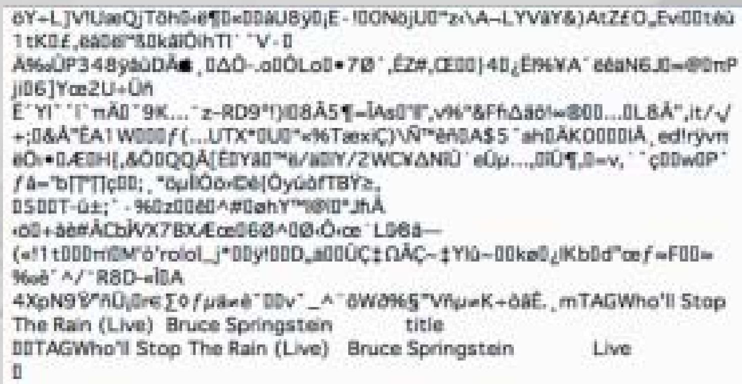
# Leggere e scrivere i TAG ID3

**Grazie a Erik Kemp sono nati i Tag ID3, sei campi che contengono informazioni su un brano. Osserveremo la loro struttura e l'applicheremo a un linguaggio di programmazione, il C.**

I Tag ID3 sono dei campi contenenti informazioni riguardanti un file di tipo MPEG 1 Layer 3, più conosciuti come MP3. Nella prima versione dei Tag (Id3v.1) questi campi sono per l'esattezza 6: titolo, autore, album, anno, commento, genere e si trovano alla fine del file audio, in chiaro. Con in chiaro voglio dire che si leggono normalmente. Provate ad aprire un mp3 con editor di testo e posizionatevi alla fine del file, noterete che ci sono delle scritte leggibili, i campi. Per modificare questi Tag però bisogna seguire una struttura ben precisa.

## >> La Struttura

Come vi ho detto prima, i Tag Id3 sono alla fine di un file, più precisamente agli ultimi 128 byte. Nel box vi ho scritto quanti byte hanno a disposizione i vari campi e in che posizione si trovano.
Ricordate che l'ordine da mantenere è questo, non potete cambiarlo. La parte Tag come vedete è separata dagli altri campi, altrimenti sarebbe sbagliato visto che non è un campo, ma serve a identificare l'inizio dello spazio dedicato ai Tag Id3 (v. 1), e il suo contenuto può solo essere la stringa "Tag". Se manca quest'ultima significa che i Tag Id3 (v. 1) non sono presenti. Altra cosa da ricordare è che c'è un campo che si differenzia dagli altri, l'anno, perché può contenere solo numeri.
Leggere e scrivere i Tag Id3 è piuttosto semplice, ma dovete avere comunque una minima conoscenza del C. Sul sito di Hacker Journal potrete trovare il sorgente di un programma che fa le stesse identiche cose che tratteremo fra poco (si chiama "simit"), anche se sarebbe meglio che lo scriveste voi. Si impara sempre di più se si scrive manualmente il codice.




Come appare un file Mp3 aperto con un editor di testi. In fondo, si notano le informazioni dei tag Id3.

## >> Leggere i tag

Avremo bisogno di un array di char, di un file pointer e di un contatore per la funzione for che faremo in seguito.

```
FILE *fp;
int cont;
char buff[129]

fp=fopen("mymp3.mp3", "rb");
fseek(fp, -128, SEEK_END);
```

Con questo pezzetto di codice apriamo il file "mymp3.mp3" e ci posizioniamo 128 byte prima della fine del file. Ora abbiamo due possibilità per leggere i campi: la prima è quella di leggere

### LA POSIZIONE DEI TAG

| Campo | byte | Posizione |
|---|---|---|
| TAG | 3 byte | 0..2 |
| Titolo | 30 byte | 3..32 |
| Autore | 30 byte | 33..62 |
| Album | 30 byte | 63..92 |
| Anno | 4 byte | 93..96 |
| Commento | 30 byte | 97..126 |
| Genere | 1 byte | 127..127 |

### I GENERI PRINCIPALI

| Hex | ASCII | Genere |
|---|---|---|
| 03 | [03] | Dance |
| 07 | [07] | Hip-Hop |
| 09 | [09] | Metal |
| 0D | [13] | Pop |
| 0F | [15] | Rap |
| 12 | [18] | Techno |
| 23 | [35] | House |
| 18 | [24] | Soundtrack |



A proposito di estensioni del formato, ecco tutte le informazioni che possono essere inserite in un brano dal lettore Mp3 iTunes di Apple; non è detto però che queste informazioni possano essere lette da tutti i lettori di altre marche.

un campo alla volta e di memorizzarlo in variabili diverse, la seconda (quella che useremo) è quella di leggere i 128 byte e memorizzarli in una sola variabile. In questo caso come funzione useremo la fread.

```
fread(buff, 1, 128, fp);
```

Controlliamo se è presente la stringa "TAG", e se non c'è lo segnaliamo all'utente e usciamo.

```
 if(strncmp(buff, "TAG", 3)) {
  printf("\nTag ID3 mancanti!\n");
  exit(-1);
}
```

Adesso dobbiamo solo leggere il contenuto dei campi dalla variabile "buff". Per questo useremo la funzione "for", quindi con vari cicli scriveremo sullo standard output (il monitor) carattere per carattere il titolo. Per scrivere gli altri campi fate riferimento allo schema della struttura.

```
printf("\nTitolo: ");
for(i=3; i<=32; i++) {
 if((buff[i]==' ')&&(buff[i+1]==' ')) break;
 else printf("%c", buff[i]);
}
```

L'if serve per evitare cicli inutili, perché se il titolo (o qualsiasi altro campo) è meno di 30 caratteri, il resto dello spazio va riempito con degli spazi.

## >> Scrivere i tag

Scrivere i campi è quasi più facile che leggerli, quindi iniziamo col scrivere il titolo, il resto sta a voi.

Iniziamo col dichiarare il file pointer, la variabile che conterrà il titolo e quella che conterrà l'identificatore, poi come prima ci spostiamo 128 byte prima della fine del file, leggiamo 3 caratteri e controlliamo se corrispondono alla stringa "TAG". Se non dovessero corrispondere scriveremo noi la stringa.

```
 FILE *fp;
 char titolo[30], tag[3];

 fp=fopen("mymp3.mp3", "ab");
 fseek(fd, -128, SEEK_END);
 fread(tag, 1, 3, fp);
 if(strncmp(tag, "TAG", 3)) fwrite("TAG", 1, 3, fp);
```

Ora chiediamo all'utente di inserire il titolo che scriveremo. Prima di scrivere però dobbiamo posizionarci 125 byte prima della fine del file, o più semplicemente 3 byte dopo la nostra posizione corrente.

```
printf("\nInserire il titolo: ");
fgets(titolo, 30, stdin);
fseek(fp, 3, SEEK_CUR);
if(strlen(titolo)<30) {
 int i;
 for(i=strlen(titolo); i<=30; i++) titolo[i]=' ';
 }
fwrite(titolo, 1, 30, fp);
```

Se il titolo che ci ha dato l'utente è meno di 30 caratteri, dobbiamo riempire lo spazio che avanza con degli spazi (con il ciclo for). Ora non ci resta che chiudere il file e il gioco è fatto!

## >> Il Genere

Per modificare il genere dobbiamo cambiare l'ultimo byte del file mp3 con un carattere. Per comodità nel codice non chiederemo all'utente il carattere, ma bensì il codice ASCII.

Quello che dobbiamo fare adesso è molto semplice, chiediamo il codice all'utente, ci posizioniamo all'ultimo byte e scriviamo il genere.

```
 Int code;

[…]

 printf("Inserire il codice ASCII del genere: ");
 scanf("%d", &code);
 if((code>146)||(code<0)) {
  printf("Errore: Codice Errato!\n");
  exit(-1);
 }
 fseek(fp, -1, SEEK_END);
 fprintf(fp, "%c", code);
```

Con l'if controlliamo che il codice immesso dall'utente sia valido, per cui non deve superare i generi (che sono 146 partendo da 0) e non deve essere minore di 0. Volendo si può dare il codice anche in esadecimale, ma in questo caso al codice bisognerebbe anteporre "0x". Per esempio, se volete il genere pop scrivete "13" oppure "0x0d". Nel box troverete qualche genere, ma una lista completa (di tutti i 147 generi) è insieme al sorgente di Simit.

Se vi interessa potete trovare molte informazioni sul sito ufficiale del Tag Id3, www.id3.org.

**norloz**

## LE EVOLUZIONI DEGLI ID3

Questo articolo si riferisce alla prima versione dei Tag Id3, la v.1. Già ai tempi della sua introduzione, questa versione ha presentato molti limiti: per esempio, non prevedeva un campo per specificare il numero di traccia del CD da cui il brano era stato estratto. La prima modifica (v1.1) conisisteva proprio nell'introduzione di questo tipo di informazione. Altre ne vennero aggiunte inserendo codici particolari nel campo dei commenti, ma non tutti i programmi usavano questo campo nello stesso modo. Rimaneva inoltre un importante problema: il campo per il titolo poteva contenere al massimo 30 caratteri, cosa che poteva causare qualche problema con titoli come "Elderly woman behind the counter in a small town, Live a Verona giugno 2000".

La versione 2 ha messo un po' di ordine nel caos, inserendo molti altri campi, ed estendendo molti limiti. L'attuale versione (v2.4) può addirittura includere altri file (foto della copertina del disco, testo eccetera), e può teoricamente raggiungere la dimensione di 256 Megabyte.

# INTRODUZIONE ALLA PROGRAMMAZIONE

**Prima di imparare un linguaggio, bisogna capire i concetti che stanno alla base della programmazione: facciamo conoscenza con gli algoritmi.**

Molti pensano che i computer siano macchine estremamente intelligenti e superiori all'uomo. In realtà le cose non stanno proprio in questi termini; i computer hanno il grande vantaggio di poter eseguire, in pochi secondi, operazioni che all'uomo richiederebbero anni (se si è molto veloci!); quindi la loro prima qualità è la velocità. Inoltre hanno la capacità di non annoiarsi e stancarsi nel ripetere ciclicamente le stesse operazioni o operazioni poco dissimili.
Ma per far questo il computer deve essere istruito passo passo dall'uomo.
Questo processo di insegnamento va sotto il nome di programmazione. Quello che cercheremo di fare in questa serie di articoli è fornire i rudimenti di quest'arte, senza riferirsi a uno specifico linguaggio. Starà poi al singolo lettore **approfondire ed ampliare gli argomenti trattati** secondo quelli che sono i suoi interessi e le sue esigenze.

## >> Che linguaggio parli?

Il primo problema che si è dovuto affrontare è stato quello di far comunicare l'uomo con la macchina; si è dovuto cercare un compromesso fra quello che è il linguaggio articolato, complesso e non universale dell'uomo, con il linguaggio semplice e monotono del computer, ossia il **linguaggio macchina costituito da una serie di 0 e 1** (acceso-spento, si-no…).
La soluzione a questo problema non è unica (per fortuna o per sfortuna), e sono nati così i **vari linguaggi di programmazione, ognuno con le sue caratteristiche**, con i suoi pro e i suoi contro.
In informatica si è soliti dividere questi linguaggi in linguaggi di basso livello, come **l'assembly**, molto vicino al linguaggio macchina, e linguaggi di alto livello, come **il pascal, il basic e il fortran**, molto più vicini al linguaggio umano.
Categoria intermedia è riservata al **linguaggio C**, che viene definito un linguaggio di medio livello.
Ogni linguaggio ha le sue regole sintattiche e grammaticali e le sue parole chiave, un po' come le varie lingue.
Si può rispondere alla domanda: **"qual è il miglior linguaggio?"**.
Assolutamente no!
Ogni linguaggio nasce ed è stato sviluppato per risolvere particolari esigenze, e quindi esprimerà il massimo della sua potenza e versatilità in quel determinato campo.



## LINGUAGGI COMPILATI E INTERPRETATI

Una volta che abbiamo scritto il nostro programma, abbiamo creato quello che è definito il codice sorgente; per far questo ci siamo avvalsi di un linguaggio di programmazione, generalmente un linguaggio ad alto livello perché più vicino al linguaggio umano.
A questo punto dobbiamo tradurre il codice sorgente in un linguaggio che sia comprensibile al computer, ossia dobbiamo tradurre il nostro programma in linguaggio macchina.
Per far questo ci affidiamo ad un compilatore, che ha proprio il compito di "tradurre" il programma.
Quindi il compilatore come input (dato di ingresso) necessita del codice sorgente e come output (risultato in uscita) ci restituisce un eseguibile. Una volta ottenuto un eseguibile, mandiamo in esecuzione tale programma, che non rilegge più il codice sorgente, ma è diventato una struttura a sé stante e non necessita più di un interprete.

**LINGUAGGI COMPILATI SONO IL C, IL C++, IL FORTRAN, IL COBOL, IL PASCAL.**

Il basic è sia un linguaggio compilato che un linguaggio interpretato.
I linguaggi interpretati per essere mandati in esecuzione, hanno bisogno di un programma che permetta una "traduzione istantanea" del codice. Ogni volta che il codice deve essere eseguito, deve anche essere re-interpretato:

1) Lettura riga del codice
2) Controllo sintassi
3) Traduzione
4) Esecuzione

**TIPICAMENTE I LINGUAGGI INTERPRETATI SONO: IL PERL, LISP, IL PYTHON**

In sostanza usando un linguaggio compilato (maggiore velocità di esecuzione), per distribuire il nostro programma, daremo un eseguibile che non è facilmente modificabile, in quanto in generale non è decompilabile; mentre se usiamo un linguaggio interpretato quello che forniremo saranno i sorgenti che sono facilmente modificabili in quanto leggibili in chiaro.

**LINGUAGGIO A CODICE P**

Forma intermedia fra l'interpretato e il compilato è il java; infatti non si ha una vera e propria compilazione per tale linguaggio, ma viene generato un bytecode che ha la proprietà di poter girare su ogni sistema operativo per mezzo della Java virtual machine (JVM) che può esser vista come un interprete. Si parla in questi casi di pseudocodice o codice P.
Alcuni autori in tale tipologia di linguaggi introducono anche il python.



Certo, come nel mondo ci sono lingue più importanti di altre, come l'inglese, così anche in campo informatico ci sono linguaggi più "utili" di altri, come ad esempio il linguaggio C.

## >> Quale linguaggio conviene imparare?

Anche qui **la risposta non è unica**, e non ho la presunzione di fornirla io. Per questo citerò un mostro sacro della comunità hacker come Eric Raymond (quello del "How to become a hacker" e del "Jargon File" tanto per capirci) [HJ n°23 pag. 13] e un esperto come Chirillo (autore di "Hacker: l'attacco" e "Hacker la difesa").
Raymond nel succitato "How to become a hacker" consiglia come linguaggi: il **Python** [HJ n°15 pagg. 29-31] per iniziare, definisce il **Java** [HJ n°25-26-27, pagg. 28-31] come un altro buon linguaggio per cominciare, ma definisce il **C** come linguaggio serio per la programmazione, segue poi il **C++** [HJ n°29 pagg. 28-31], il **Perl** [HJ n°18 pagg. 28-30] ed infine include anche il **LISP**.
Chirillo in "Hacker l'attacco" individua il **linguaggio C**, il **Visual Basic**, **l'assembler** e il **Perl**.
Noi nel corso di questi articoli tratteremo il Pascal, Visual Basic e il linguaggio C.
Il Pascal sostanzialmente perché è un linguaggio molto diffuso a livello didattico (scuole superiori e corsi universitari di fondamenti di informatica); il Visual Basic perché è tutto sommato abbastanza diffuso, non è molto complesso e con poche linee di codice permette di realizzare programmi interessanti e dal gradevole aspetto grafico (anche se è limitato al solo sistema operativo Windows). Tutti questi fattori possono dare soddisfazione al principiante, incoraggiandolo a studiare sempre in maniera più profonda la programmazione. Il linguaggio C, come abbiamo visto, è ritenuto molto potente e ad ampio spettro.
Comunque, come dice Raymond: "…devi essere conscio che non raggiungerai i livelli di abilità di un hacker o più semplicemente di un programmatore se conosci solamente uno o due linguaggi - hai bisogno di imparare a **pensare ai problemi legati alla programmazione in maniera più generale, indipendentemente dal linguaggio specifico**. Per essere un vero hacker, hai bisogno di arrivare al punto di poter apprendere un nuovo linguaggio in pochi giorni, semplicemente confrontando il manuale con quanto già sai. Questo significa che dovrai imparare parecchi linguaggi differenti tra loro."

## >> Ma cos'è la programmazione?

Cerchiamo innanzitutto di capire in che cosa consiste un programma, o meglio l'algoritmo. **L'algoritmo** non è altro che una sequenza di istruzioni, e costituisce la "logica" del programma.
Durante la giornata, ognuno di noi senza accorgersene esegue una serie di algoritmi più o meno complessi.
Facciamo un esempio. Rilassiamoci un attimo e beviamoci un buon caffè, un'azione banale che compiano anche più

volte al giorno; ma **analizziamo passo passo tutto quello che compiamo quando ci prendiamo una tazzina di caffè**.

1) Prendiamo la tazzina.
2) Prendiamo la caffettiera.
3) Versiamo il caffè nella tazzina
4) Ci fermiamo quando il caffè ha raggiunto il livello desiderato.
5) Aggiungiamo lo zucchero; sappiamo dalle esperienze precedenti (interrogando la nostra memoria) quale è il numero di cucchiaini di zucchero necessari per dolcificare il caffè al punto giusto.
6) Giriamo il caffè con un cucchiaino.
7) Assaggiamo il caffè: qualora ci risulti amaro possiamo ricollegarci al punto 5, aggiungere dell'altro zucchero, girando e assaggiando nuovamente il caffè.
8) Beviamo infine (finalmente!) il caffè.

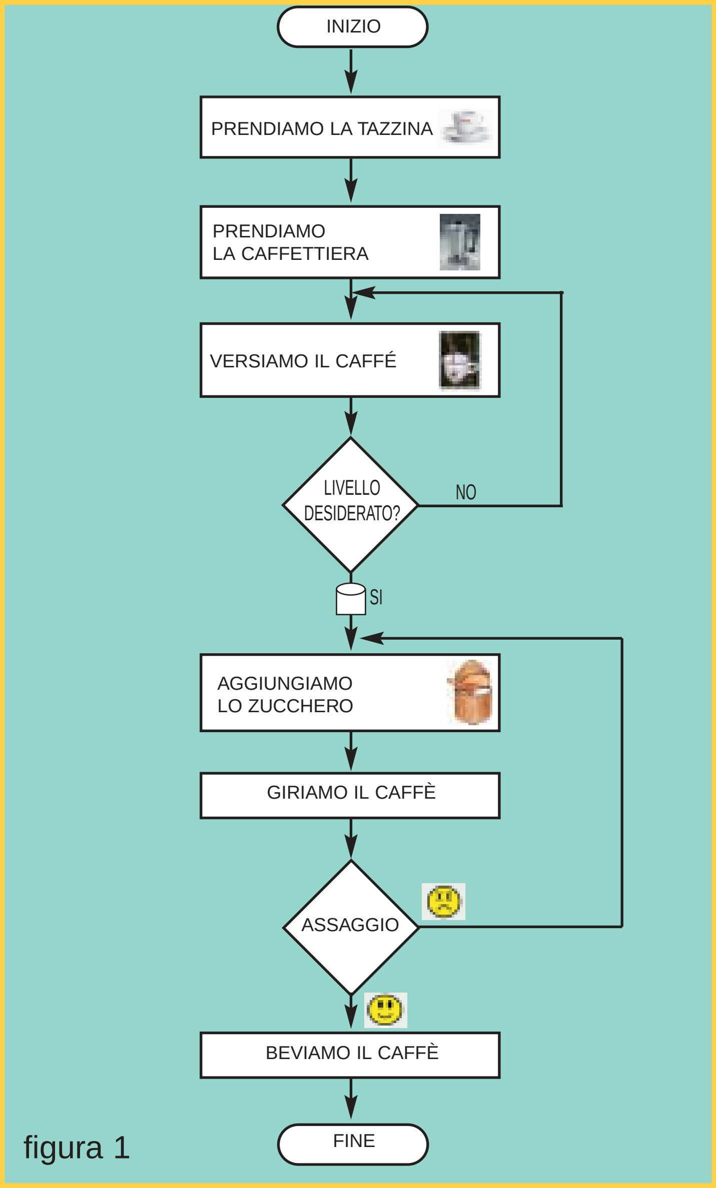


figura 1

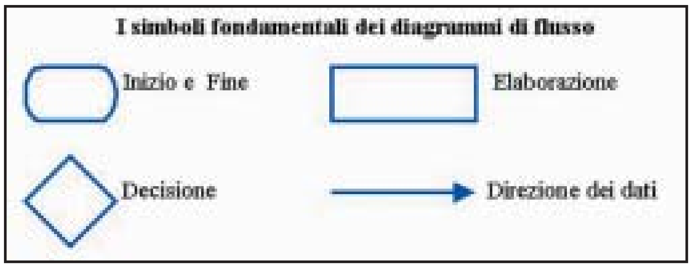
Avete visto quante operazioni ci sono dietro una semplice azione come prendere una tazzina di caffè!
A tale sequenza di operazioni possiamo dare una più efficace rappresentazione grafica, attraverso quello che in informatica viene indicato come **diagramma di flusso**. (vedi figura 1).
In tale sequenza di operazioni, possiamo distinguere tra **operazioni di elaborazione** (rettangolari) e operazioni di **valutazione di condizioni** (romboidali).
Prendere la tazzina e la caffettiera sono operazioni che in realtà appartengono alla stessa **classe** di operazioni (prendere un oggetto) ma vengono applicati a **oggetti** differenti (tazzina e caffettiera).
Tenete a mente questo concetto, perché più avanti (nei seguenti articoli) ci torneremo.
Dobbiamo quindi versare il caffè, e mentre versiamo dobbiamo **valutare il giusto livello di caffè**. Ci troviamo di fronte a un bivio e faremo delle determinate operazioni a seconda dell'esito della valutazione.
Aggiungiamo lo zucchero, andando implicitamente ad interrogare la memoria (memoria intesa come l'hard disk di un computer, ossia memoria fissa e non come una RAM che è una memoria volatile) per sapere quanti cucchiaini sono necessari a dolcificare il caffè.
Segue poi una operazione di **elaborazione** in cui sciogliamo lo zucchero nel caffè.
Iniziamo quindi a bere il caffè; in tale fase **valutiamo** (condizione romboidale) se il sapore è giusto oppure no; infatti potrebbe risultare amaro (incominciate ad aprire la mente a tutti gli imprevisti che possono succedere; perché state sicuri succederanno, lo dice la legge di Murphy!) e di conseguenza dobbiamo aggiungere dell'altro zucchero e rimescolare, ripetendo più volte tale operazione (tecnicamente **stiamo realizzando un ciclo**) fino a quando non ha raggiunto il sapore giusto o ci siamo accontentati e quindi decidiamo di berlo.

## >> Sviscerare il problema

Creare una rappresentazione tipo diagrammi di flusso, significa **aver analizzato e scomposto il problema in tanti sotto problemi più o meno dettagliati**; infatti potremmo senz'altro ampliare e dettagliare meglio l'operazione "prendi oggetto", oppure l'operazione "versare".
Una volta che abbiamo ottenuto un diagramma di flusso, siamo pronti a implementare e a tradurre l'algoritmo nel linguaggio che preferiamo, o che rende più facile l'implementazione della sequenza di istruzioni da fornire al calcolatore. Non è detto infatti che tutti i linguaggi comprendano autonomamente le funzioni che vi servono. Quindi, certi linguaggi necessitano di linee di codice aggiuntive per trattare problemi non specifici per le loro caratteristiche, e quindi di maggiori dettagli nella scomposizione del problema.
Altro punto cruciale che va tenuto presente è la **generalizzazione del problema**.
In teoria noi avremmo risolto il problema di prendere un caffè, ma una volta risolto tale problema, dobbiamo vedere se è possibile generalizzare, nel nostro caso per prendere un qualsiasi liquido.
È chiaro che facendo questo, aumentano i casi che prendiamo in esame e quindi aumenteranno anche le linee di codice che

dovremmo scrivere (si dovrà porre una condizione che eviti l'assunzione di liquidi nocivi ad esempio), **e aumenterà anche la possibilità che non tutto il codice scritto venga ogni volta eseguito** (in base alle condizioni che imponiamo).
Passando dal dover trattare solo il caffè al dover trattare una serie di liquidi, quello che abbiamo ottenuto è un aumento di quelle che in informatica vengono definite **le variabili del problema** (e quindi del programma).
Il nostro codice quindi ben presto inizia ad ingrandirsi e a diventare sempre più complesso, e **se non utilizziamo una serie di accortezze diventa facile perdere la bussola,** e perderci all'interno della nostra creatura, non riuscendo bene a capire il flusso all'interno del codice.

## CAPIRE I DIAGRAMMI DI FLUSSO




### INIZIO E FINE
Identificano il primo e l'ultimo passo del diagramma di flusso.

### ELABORAZIONE
Qualsiasi operazione fatta con i dati in possesso del programma, e che non richiede scelte o decisioni.

### DECISIONE
Scelta tra due o più condizioni, solitamente di tipo "vero o falso". Il programma in questo punto si biforca, e può compiere operazioni diverse a seconda della condizione impostata.

### DIREZIONE DEI DATI
Indica il flusso del programma e ne facilita la comprensione.




### DATI IN/OUT
Usato per rappresentare dati che devono essere acquisiti dal programma, o che il programma visualizza all'utente.

### INPUT MANUALE
Dati che l'utente deve inserire manualmente

### DOCUMENTO
Un qualsiasi file, che può essere aperto o prodotto dal programma.

### DISCO MAGNETICO
Il supporto di memorizzazione predefinito

### MEMORIA AD ACCESSO DIRETTO
Può essere la memoria RAM, o altri tipi di memoria ad accesso casuale.

### INIZIALIZZAZIONE
Qui viene attribuito un valore alle variabili del programma. Ne parleremo nel prossimo numero.

## >> Consigli per una buona programmazione

Quasi ogni linguaggio di programmazione prevede la possibilità di **inserire dei commenti** tra un blocco di istruzioni e un altro. I commenti sono brevi testi che descrivono le operazioni in un linguaggio comprensibile da un altro programmatore, o persino da sé stessi, se si dovesse riprendere in mano il programma dopo un certo periodo di tempo. Infatti nel momento in cui realizzate il programma tutto vi sembra chiaro, ma se provate a riprendere in mano il codice scritto da voi (di una certa complessità), **a distanza di breve tempo, la lettura risulterà più difficoltosa**.
Solitamente, i commenti rispecchiano i punti principali del diagramma di flusso, e precedono le istruzioni di programmazione a cui si riferiscono.
È buona norma commentare il più possibile i programmi; anche se a prima vista potrebbe risultare alquanto noioso, in realtà ciò è estremamente utile perché facilita la lettura sia a voi che a terze persone che potrebbero avere accesso al vostro codice sorgente.
Ogni linguaggio avrà una sua sintassi per poter inserire i commenti, ma sarà lievemente diverso da caso a caso.
Inoltre, sempre per facilitare la lettura del codice, è utile scriverlo con una opportuna tabulazione (che nel gergo informatico prende il nome di **indentazione del codice**), in modo che risultino chiari ed evidenti a prima vista i vari blocchi costituenti il programma e l'apertura e chiusura di una serie di istruzioni. Ma questo lo vedremo meglio più avanti.

## >> Nel prossimo articolo...

Nel prossimo articolo vedremo meglio cosa si intende per variabili e per costanti; quali sono le varie tipologie di variabili e come dichiararle.

**>>>----Robin---->**
**RobinHood.Sherwood@libero.it**

## LINK UTILI

La home-page di Steven Eric Raymond:
http://www.catb.org/~esr/

How to become a hacker (in italiano):
http://www.saprionline.com/gratis/informatica/hacker-howto-it.html

The Jargon File ver 4.4.2:
http://catb.org/~esr/jargon/

Le leggi di Murphy:
http://www.sitopreferito.it/html/leggi_di_murphy.html

Le leggi di Murphy sui computer:
http://spazioinwind.libero.it/psicoinfo/murphy.htm